

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

Факультет електроніки

(повна назва інституту/факультету)

Кафедра звукотехніки та реєстрації інформації

(повна назва кафедри)

«На правах рукопису»

УДК 623.6

«До захисту допущено»

Завідувач кафедри

_____ (Власюк Г.Г.)
(підпис) (ініціали, прізвище)

“ ____ ” _____ 2018 р.

Магістерська дисертація

зі спеціальності 171 Електроніка

(код і назва)

на тему: «Засоби розширеного радіусу дії із застосуванням технології Wi-Fi для
знешкодження вибухонебезпечних предметів».

Виконав: студент VI курсу, групи ДВ-72 мп
(шифр групи)

Коротков Іван Геннадійович

(прізвище, ім'я, по батькові)

(підпис)

Науковий керівник _____ доцент, к.т.н., доцент Швайченко В. Б.

(посада, науковий ступінь, вчене звання, прізвище та ініціали)

(підпис)

Консультант _____

(назва розділу)

(посада, вчене звання, науковий ступінь, прізвище, ініціали)

(підпис)

Рецензент _____

(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали)

(підпис)

Засвідчую, що у цій магістерській
дисертації немає запозичень з праць
інших авторів без відповідних
посилань.

Студент _____
(підпис)

Київ – 2018 року

**Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»**

Інститут (факультет) _____ Факультет електроніки
(повна назва)

Кафедра _____ Звукотехніки та реєстрації інформації
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною
програмою

Спеціальність (спеціалізація) 171 Електроніка (Електронні та інформаційні
технології кінематографії та аудіовізуальних систем)
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ (Власюк Г.Г.)
(підпис) (ініціали, прізвище)
« ____ » _____ 2018 р.

**ЗАВДАННЯ
на магістерську дисертацію студенту
_____ Короткову Івану Геннадійовичу
(прізвище, ім'я, по-батькові)**

1. Тема дисертації: Засоби розширеного радіусу дії із застосуванням технології
Wi-Fi для знешкодження вибухонебезпечних предметів.

науковий керівник дисертації: Швайченко Володимир Борисович, к.т.н., доцент
(прізвище, ім'я, по-батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від «07» листопада 2018р. № 4114-с

2. Строк подання студентом дисертації 05.12.2018

3. Об'єкт дослідження: процеси знешкодження вибухонебезпечних предметів.

4. Предмет дослідження (Вихідні дані для магістерської дисертації за освітньо-
професійною програмою): пристрій знешкодження вибухонебезпечних
предметів з безпроводовим інтерфейсом

5. Перелік завдань, які потрібно розробити: загальна характеристика засобів для
знешкодження вибухонебезпечних предметів з дистанційним керуванням,

визначити шляхи вдосконалення засобів для знешкодження вибухонебезпечних предметів, розроблення стартап проекту, обґрунтування структури та схеми засобу розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів

6. Перелік графічного (ілюстративного) матеріалу: 34 рис., 23 таб., 1 презентація, 12 слайдів.

7. Орієнтований перелік публікацій: збірник наукових матеріалів XXIV Міжнародної науково-практичної інтернет-конференції el-conf.com.ua «Новини науки XXI століття» частина 13, Перша всеукраїнська науково-технічна конференція «Сучасні технології кіно та аудіовізуальних систем».

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання 15 вересня 2017 року.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів дисертації	Примітка
1	Робота над першим розділом	13 квітня 2018 р.	
2	Робота над другим розділом	5 травня 2018 р.	
3	Робота над третім розділом	21 вересня 2018 р.	
4	Робота над четвертим розділом	15 листопада 2018 р.	
5	Оформлення пояснювальної записки	3 грудня 2018 р.	

Студент

(підпис)

Коротков І. Г.

(ініціали, прізвище)

Науковий керівник дисертації

(підпис)

Швайченко В. Б.

(ініціали, прізвище)

РЕФЕРАТ

Магістерська дисертація: 87 с., 34 рис., 23 табл., 2 дод., 18 джерел.

**ЗАСОБИ ЗНЕШКОДЖЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ,
СИНТЕЗ, ПРОГРАМНІ ЗАСОБИ, ТЕХНОЛОГІЯ Wi-Fi.**

Метою проекту є розробка засобів розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів. Дані засоби є важливою частиною саперного комплексу технічного оснащення, що може бути корисним в роботі по розмінуванню в місцях військових конфліктів. Даний прилад може становити інтерес для військових, ДСНС, піротехніків, а також використаний під час навчань.

Об'єктом дослідження є процес розробки засобів розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів

У даній дисертації проведено аналіз підривних машинок та піропультів, які використовуються наразі, що дозволило визначити оптимальний та надійний функціонал системи. Для реалізації приладу проведено аналіз та вибір сучасної елементної бази, на основі якої розроблено схему електричну принципову. Визначено основні параметри, діапазон та шляхи прокращень.

SUMMARY

Master's dissertation: 87 pages, 34 pictures, 23 tables, 2 copies. 18 sources.

MEANS OF DISPOSAL OF EXPLOVISE OBJECTS, SYNTHESIS, SOFTWARE, WiFi TECHNOLOGY.

The purpose of the project is to develop expanded range of devices using Wi-Fi technology to eliminate explosive objects. These facilities are an important part of the engineering equipment complex, which may be useful in mine clearance in places of military conflict. This device can be of interest to the military, DNS, pyrotechnics, and also used during exercises.

The object of the study is the development of expanded range products using the Wi-Fi technology for the clearance of explosive objects

In this dissertation, an analysis of the blasting machines and pyropults that are used at present is carried out, which made it possible to determine the optimal and reliable functional of the system. For implementation of the device the analysis and the choice of the modern element base, on the basis of which the scheme of electrical principles has been developed. The basic parameters, range and ways of perverts are determined.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	8
ВСТУП.....	9
1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЗАСОБІВ ДЛЯ ЗНЕШКОДЖЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ З ДИСТАНЦІЙНИМ КЕРУВАННЯМ	
1.1. Засоби для знешкодження вибухонебезпечних предметів.....	12
1.1.1. Способи підриву.....	12
1.1.2. Пристрій для електричного підривання	13
1.1.3. Електродетонатори	13
1.1.4. Електровибухова мережа	13
1.2. Принципи роботи засобів для знешкодження вибухонебезпечних предметів.....	19
1.2.1. Використання частот.	19
1.3. Пульт дистанційного керування.....	20
1.4. Антени.	22
1.5. Ретранслятори.....	24
1.6. Безпроводові мережі.....	24
1.6.1. Технологія безпроводної передачі даних BlueTooth.....	25
1.6.2. Технологія безпроводної передачі даних Wi-Fi.	28
1.6.3. Технологія безпроводної передачі даних ZigBee.	30
1.7. Wi-Fi модулі.	31
1.7.1. Мікроконтролер ESP-8266.	31
1.7.2. Модуль WizFi220	33
1.7.3. Модуль CC3000.....	34
1.7.4. Модулі RN та MRF.	36
1.7.5. Модуль WGM110.....	38
1.7.6. Модуль AMW007.....	39
1.7.7. Модуль WF121.	40

2. ШЛЯХИ ВДОСКОНАЛЕННЯ ЗАСОБІВ ДЛЯ ЗНЕШКОДЖЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

2.1. Особливості засобів розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів42

2.2. Визначення параметрів засобів для знешкодження вибухонебезпечних предметів, що можливо покращити.....47

2.2.1. Визначення відносної важливості основних параметрів.....48

2.2.2. Визначення діапазону покращення основних параметрів.....49

2.2.3. Формування задач досліджень.....49

3. РОЗРОБЛЕННЯ СТАРТАП ПРОЕКТУ

3.1. Опис ідеї проекту.....52

3.2. Технологічний аудит ідеї проекту 53

3.3. Аналіз ринкових можливостей запуску стартап проекту 54

3.4. Розроблення ринкової стратегії проекту 60

3.5. Розроблення маркетингової програми стартап проекту 63

4. ОБГРУНТУВАННЯ СТРУКТУРИ ТА СХЕМИ ЗАСОБУ РОЗШИРЕНОГО РАДІУСУ ДІЇ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ Wi-Fi ДЛЯ ЗНЕШКОДЖЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

4.1. Обґрунтування структурної схеми пристрою.....65

4.2. Обґрунтування та вибір елементної бази.....66

4.3. Особливості схеми електричної принципової.....68

4.4. Програмна реалізація та моделювання роботи системи.....72

4.4.1. Обґрунтування алгоритму роботи програми.....72

4.4.3. Опис роботи програмного забезпечення засобу для знешкодження вибухонебезпечних предметів73

4.5. Особливості друкованої плати для засобу знешкодження вибухонебезпечних предметів.....75

4.5.1. Вибір типу друкованої плати.....76

4.5.2. Вибір матеріалу друкованої плати.....76

4.5.3. Виготовлення друкованих плат.....76

ВИСНОВКИ.....	80
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.....	82
ДОДАТОК А.....	84
ДОДАТОК В.....	88

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

- АЦП – аналогово – цифровий перетворювач;
ДП – друкована плата;
ЕВМ – електровибухова мережа;
ЕД – електродетонатор;
ЗВНП – знешкодження вибухонебезпечних предметів;
ІЧ – випромінювання – інфрачервоне випромінювання;
МК – мікроконтролер;
ПДК – пульт дистанційного керування;
ЗЗВНП – засоби знешкодження вибухонебезпечних предметів;
САПР – система автоматизованого проектування.

ВСТУП

В час розповсюджених військових конфліктів, є актуальною тема розробки технічних заходів, що спрямовані на подолання наслідків проведення бойових дій, а саме – знешкодження не спрацювавших боєприпасів на територіях з цивільним населенням. З розвитком сучасних технологій є не раціональним використання застарілих підривних машинок, що є дуже габаритними, натомість кращим варіантом є використання малогабаритних мікроконтролерних збірок та безпроводних технологій, наприклад Wi-Fi.

Використання технології Wi-Fi є доцільним, тому що можливе керування пристроєм з будь-якого пристрою з Wi-Fi модулем, а це смартфони, ноутбуки, планшети, тощо. Також такі пристрої не потребують великих антен, за рахунок короткої довжини хвилі.

Функціонування засобів дистанційного знешкодження вибухонебезпечних предметів засновується на принципі передачі сигналу з командно-передавального пристрою на приймально-виконавчий пристрій, що ініціює імпульс струму на електродетонатор.

Найбільш важливими критеріями пристроїв є дальність дії та розміри. В даному випадку доцільно використовувати потужні приймально-передавальні пристрої та намагатися зменшити розміри пристрою.

Однією з основних характеристик пристрою знешкодження вибухонебезпечних предметів є надійність. Тому обрано мікроконтролер, який має копію основних параметрів роботи системи в незалежній пам'яті, велику кількість виводів і т.д. Крім контролера пристрій знешкодження вибухонебезпечних предметів включає в себе модуль Wi-Fi, антену та набір реле.

Дистанція нормальної роботи пристроїв залежить від потужності передавача, наявності антен, підсилювачів, повторювачів, рельєфу та геомагнітної обстановки. Мінусом використання технології Wi-Fi є невелика дальність дії, що можна виправити, додав у лінію повторювачі та потужнішу антену.

В мікроконтролерах з Wi-Fi модулем, наприклад лінійка ESP компанії Espressif, використовуються друковані антени, що працюють на відстанях до 350 м, але задля розширення радіусу дії можливо встановити зовнішню додаткову антену, що збільшує робочу відстань до 480 м. Також можливо використовувати в лінії передачі додаткові пристрої, що будуть приймати керуючий сигнал та передавати його на кінцевий пристрій.

Ще одним фактором актуальності та доцільності використання пристроїв з мікроконтролерами та безпроводними технологіями, є можливість об'єднання їх в одну мережу, що надає змогу активувати їх в будь-якому порядку, та в будь-який час. Також один кінцевий пристрій може мати кількість виходів, яку потребує поставлена задача.

Розповсюдженість мікроконтролерів на ринку дає широкий вибір, низьку вартість та достатню їх надійність. Вартість такого типу приладів не буде набагато перевищувати вартість застарілих підричних машинок.

Принцип роботи полягає в тому, що пристрій виступає в ролі сервера та містить в своїй пам'яті виконавчу програму, керування відбувається дистанційно зі смартфона, ноутбука, або планшета, методом підключення до сервера, та запуску програми, після чого пристрій подає імпульс струму на обраний вихід та ініціює електродетонатор.

Аналіз ринку показав, що на ньому представлений вузький асортимент пристроїв знешкодження вибухонебезпечних предметів, більшість з яких застраліла, а також відсутні рішення з безпроводним керуванням.

Засоби розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів можуть використовуватися задля перевірки нового електровибухового обладнання (електродетонаторів), також не тільки в військовій справі, а й у цивільних піротехнічних заходах, запуску феєрверків, перевірці протипожежного обладнання, тощо.

Метою даної магістерської дисертації – є розробка засобів розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів, у якій перш за все вирішувалось питання

створення нового типу пристроїв, шляхом поєднання вибухових машинок та пристроїв дистанційного керування, а також збільшення радіусу дії таких пристроїв.

Завданням є дослідження визначення доцільності та реалізація безпроводового інтерфейсу дистанційного керування пристроєм для знешкодження вибухонебезпечних предметів на безпечній відстані.

1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЗАСОБІВ ДЛЯ ЗНЕШКОДЖЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ З ДИСТАНЦІЙНИМ КЕРУВАННЯМ

1.1 Засоби для знешкодження вибухонебезпечних предметів

Засоби для знешкодження вибухонебезпечних предметів (ЗЗВНП) можна розділити на три групи за методом знешкодження:

- детонація вибухової речовини;
- руйнування вибухонебезпечного предмету;
- розбирання.

Більш безпечними методами є детонація вибухової речовини та руйнування вибухонебезпечного предмету [1]. В багатьох випадках можлива тільки детонація.

1.1.1 Способи підриву

Механізми приведення детонатора у дію можуть бути класифіковані наступним чином:

- механічного принципу дії;
- електричного принципу дії;
- електронного принципу дії;
- хімічного принципу дії;
- комбінованого принципу дії.

Механізми приведення детонатору в дію механічного принципу можуть бути розділені на обривні, натискні, розвантажувальні та натяжні [13].

Електричний спосіб підриву зарядів проводиться за допомогою електродетонаторів, джерела струму, провідників та заряду. Електронний спосіб підриву виконується дистанційно, через радіоканал. Хімічний принцип дії зазвичай заснований на дії кислот, що звільнюють шлях для ударного механізму, або хімічного займання.

1.1.2 Пристрій для електричного підривання

Вибухова машинка, підривна машинка — переносний пристрій для електричного підривання зарядів вибухової речовини (ВР) [2]. Розрізняють динамоелектричні та конденсаторні вибухові машинки. Вітчизняні типи вибухових машинок: батарейні конденсаторні прилади КВП-1/100м, ПІВ-100м; іскробезпечний високочастотний вибуховий прилад ІВП-1/12; граничні вибухові прилади КВП 200 і КВП 750.

В залежності від джерела струму розташованого всередині пристрою для електричного підривання, конденсаторні підривні машинки поділяють на індукторні (з малогабаритними генераторами), акумуляторні (з герметизованими акумуляторами малих розмірів) та батарейні (з гальванічними батареями). По типу корпусу вони поділяються на вибухобезпечні (не викликаючи займання метановмісних газів) та звичайні (призначені для середовища з відсутністю газу та пилу). Вибухобезпечні пристрої повинні забезпечувати іскробезпечність. Пристрої для електричного підривання використовують в промислових роботах та в військовій справі.

1.1.3 Електродетонатори

Найбільш поширеним є електричний спосіб підриву. Електричний спосіб підриву зарядів проводиться за допомогою електродетонаторів, джерела струму, провідників для підключення та заряду.

Електродетонатором (ЕД) є капсуль-детонатор, з'єднаний в одне ціле з електрозапальником, перетворює електричну енергію в теплову і відповідно викликає спалах запалюється складу [2]. Електродетонатори за характером дії поділяють на три групи: миттєві, уповільнені і короткосповільнені. Електродетонатори випускають трьох типів: миттєвої дії, короткосповільненої дії, сповільненої дії (рис. 1.1).

Електродетонатор містить колодочку з містком розжарювання, на яку

нанесений запалювальний склад, заряди ініціюючого і вторинного ВВ.

Всі електродетонатори, що входять в групу для підривання, повинні мати однаковий опір і бути з однієї партії.

Дія електродетонаторів заснована на нагріванні електричним струмом містка розжарювання.

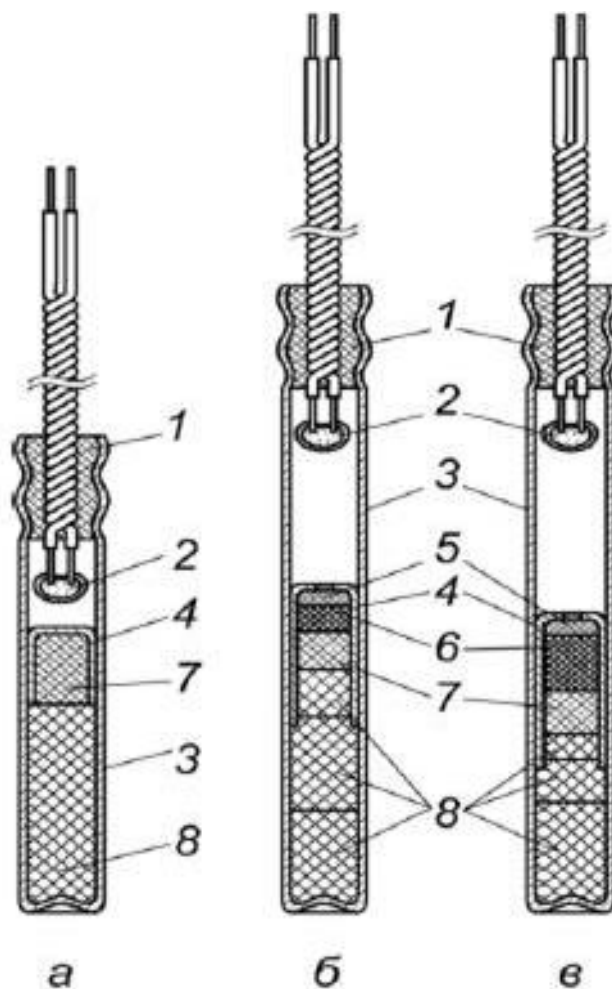


Рисунок 1.1 – Типи електродетонаторів

(а) миттєвої дії, б) короткосповільненої дії, в) сповільненої дії

1- пробка

2- запалювальна головка

3- корпус

4- втулка

5- запалювальна суміш

6- сповільнююча речовина

7- первинний заряд ВР

8- вторинний заряд ВР

Опір електродетонаторів складається з електричного опору містка і вивідних проводів в холодному стані. Даний параметр дає можливість судити про відсутність несправностей в електрозапальнику.

Займання електродетонаторів проводиться або від електричної мережі, або від вибухової машинки. Для підривання електродетонатори з'єднують послідовно, паралельно або змішано.

Чутливість електродетонатора S - величина, зворотна імпульсу займання. Номінальний імпульс займання K_n - таке його значення, яке стає практично постійним при струмі, приблизно рівному двократному значенню стомілісекундного запалювального струму. Імпульс плавлення містка - найменше значення імпульсу струму (постійного), при якому відбувається плавлення (перегоряння) містка ЕД.

У електродетонаторів миттєвої дії електрозапальник знаходиться безпосередньо у чашечки капсуля - детонатора, який при включенні струму вибухає практично миттєво. Несвоєчасне займання електродетонаторів струмами витоку (або, як їх зазвичай називають, ґрунту та блукаючих струмів) призводить до передчасного підривання.

Для подачі струму на запал електродетонатори в польових умовах застосовують провід ПСМ зі сталевими і мідними жилами діаметром 2-3 мм. Для пристрою моментальної лінії найбільш часто використовують провід ПВР.

1.1.3 Електровибухова мережа

Електровибухова мережа (ЕВМ) – у вибуховій справі сукупність електродетонаторів та проводів, що з'єднують електродетонатори між собою та джерелом струму [1].

ЕВМ складається з магістралі, що з'єднує джерело струму (або підривну машинку) з розподільною мережею, яка розподіляє струм між електродетонаторами.

Розподільну мережу складають кінцеві проводи, що йдуть від вивідних проводів електродетонаторів і дільничні (з'єднувальні) проводи, які з'єднують між собою кінцеві проводи суміжних електродетонаторів і приєднують кінцеві проводи до магістралі.

В практиці вибухових робіт застосовуються ЕВМ: послідовна — всі електродетонатори з'єднані послідовно, паралельна (паралельно-пучкова, паралельно-ступінчата, кільцева) — з паралельним з'єднанням всіх детонаторів та змішана — електродетонатори в групах з'єднані між собою одним способом, а групи між собою — іншим.

1.2. Принципи роботи засобів для знешкодження вибухонебезпечних предметів

Функціонування цього ряду пристроїв будується на передаванні сигналу з командно-передавального пристрою на приймально-виконавчий пристрій сигналу керування, що ініціює імпульс струму на електродетонатор (рис. 1.2.).

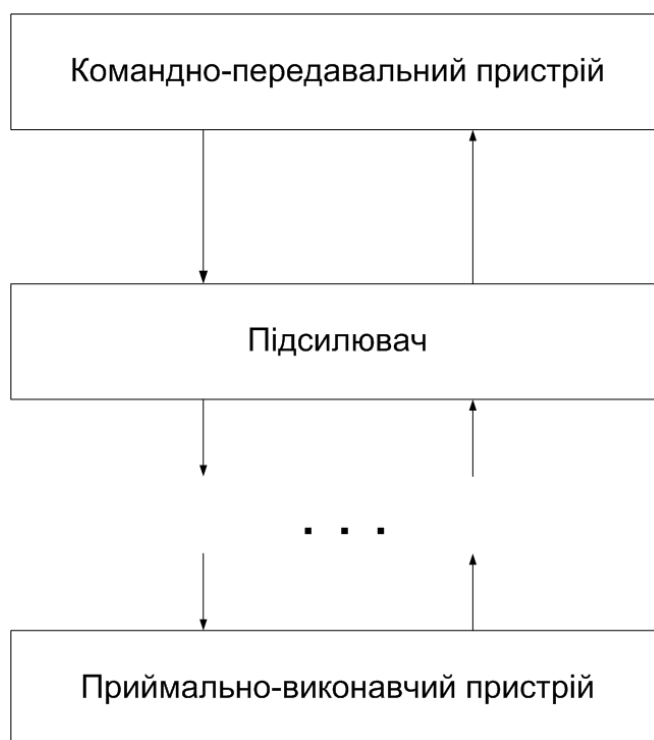
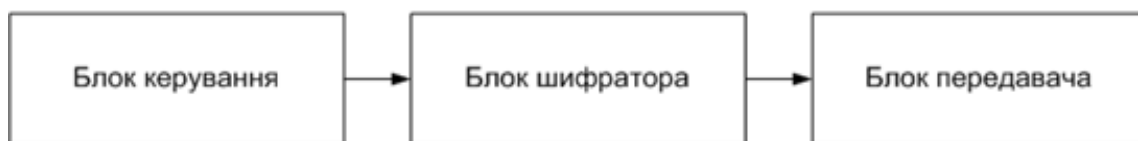


Рисунок 1.2 – Загальна схема ЗЗВНП

В загальному випадку в приймально-виконавчий пристрій входять такі елементи: блок приймача (приймає команди керування), блок дешифратора (дешифрує прийняту команду), виконавчий блок (після прийняття й дешифрування команди управління, подає імпульс струму на електродетонатор) (рис. 1.3.б).

В командно-передавальний пристрій входять: блок шифратора та блок передавача (рис. 1.3.а).



а) Командно-передавальний пристрій



б) Приймально-виконавчий пристрій

Рисунок 1.3 – Схема основних блоків пристрою

а) Командно-передавальний пристрій

б) Приймально-виконавчий пристрій

Дистанція, на якій можна використовувати пристрій залежить від потужності передавача, наявності підсилювачів у лінії зв'язку, рельєфу, геомагнітної обстановки. Щоб збільшити надійність, використовують шифрування керуючого сигналу. Також пристрої можуть мати декілька каналів на різних частотах для більшої ефективності та завадостійкості, в залежності від умов використання.

Задля перевірки доставки сигналу до кінцевого пристрою та виявлення місця проблеми у лінії, застосовують зворотній сигнал від приймально-виконавчого пристрою до командно-передавального.

1.2.1. Використання частот

В пристроях для знешкодження вибухонебезпечних предметів для зв'язку між передавальним та приймальним пристроєм можна використовувати радіоканал. По ньому передається сигнал, який несе певну інформацію, на приймальний пристрій, де він набуває форми, зручної для сприймання користувачем.. Радіосигнали можуть передаватися безперервно або циклічно, також — за сигналом-запитом.

Основними частинами системи радіоуправління є пристрої (передавачі), що надсилають через радіоканал на керований об'єкт команди (керуючу інформацію), і пристрої (приймачі), на яких приймані сигнали розшифровуються та діють на систему управління кінцевим об'єктом. Команди можуть бути неперервними та перервними.

В засобах розширеного радіусу дії для знешкодження вибухонебезпечних предметів можливо використовувати канал Wi-Fi. При цьому можна впровадити каскад повторювачів, задля збільшення дистанції, керування з пульта (командно-передавальний пристрій), керування зі смартфона, чи іншого пристрою з модулем Wi-Fi, використання 2-х частот: 2,4 ГГц та 5 ГГц.

Зазвичай використовують низькі частоти, але при використанні пристрою за межами міста, за відсутності завад у діапазоні коротких та ультракоротких хвиль, можна використовувати й діапазон каналу WiFi, задля простоти і більшої зручності. Адже простіше носити з собою смартфон, який наразі є майже в кожного, а не ще окремі пристрої. Також такі передавачі не потребують громіздких антенн, що збільшує компактність та зменшує ризики пошкодження пристрою.

Використання діапазону частот нижче 20 МГц є недоцільним через значну складність створення портативного командно-передавального пристрою, здатного ефективно функціонувати з короткими антенами.

Вибір частот слід проводити з урахуванням побутових та промислових завад.

1.3. Пульт дистанційного керування

Пульт дистанційного керування (ПДК) — електронний пристрій для віддаленого (дистанційного) керування іншим електронним пристроєм. Існують як автономні, так і неавтономні (проводові) варіанти. Конструктивно пульт — звичайно невеличка коробка, що містить в собі електронну схему, кнопки керування і (як правило) джерело автономного живлення.

ПДК використовуються для дистанційного керування як мобільних об'єктів (наприклад, БПЛА), так і апаратами і механізмами на мобільних об'єктах (літаки, космічні кораблі, судна и т. д.), також керування виробничими процесами, системами зв'язку, технікою підвищеної небезпеки.

Широко використовуються для дистанційного керування побутовими електронними приладами.

Пульти дистанційного керування розрізняють за:

- живленням:
 - автономне;
 - одержуване по кабелю;
- мобільністю:
 - вбудований;
 - ношений;
- функціональністю:
 - з фіксованим набором команд;
 - з змінним набором команд;
 - з навчанням набору команд;

- каналом зв'язку:
 - механічний;
 - провідний;
 - радіоканал;
 - ультразвукової;
 - інфрачервоний.

Зазвичай в пультах використовується одна частота модуляції носія - на неї налаштований і пульт, і приймач. Частоти модуляції зазвичай стандартні - це 36 кГц, 38 кГц, 40 кГц (Panasonic, Sony).

Рідкісними вважаються частоти 56 кГц (Sharp). Фірма Bang & Olufsen використовує 455 кГц, що є великою рідкістю. Використання приймача з частотою модуляції, що неточно збігається з частотою передавача, не означає, що він не прийматиме - прийом залишиться, але його чутливість може дуже сильно впасти.

Передача сигналу здійснюється випромінюванням ІЧ-світлодіода з відповідною частотою модуляції. Для частот від 30 до 50 кГц зазвичай використовуються світлодіоди з довжиною хвилі 950 нм, а для 455 кГц - спеціальні світлодіоди з довжиною хвилі 870 нм (на цю довжину хвилі і високу частоту модуляції орієнтовані спеціалізовані приймачі TSOP5700 і TSOP7000).

Кілька таких модульованих передач і гасінь (пачок імпульсів) формують кодоване повідомлення. Приймач ІЧ-сигналу складається з декількох каскадів підсилювачів і демодулятора (частотного детектора) і чутливий до сигналу до -90 дБ (більшість електронних схем мають чутливість до -60 дБ). Також практично всі вироблені серійно ІЧ-приймачі мають ІЧ-світлофільтр (темно-червона лінза або пластина). Сам модуль ІЧ-приймача має всього три виходи: живлення, земля, вихід даних.

Для розпізнавання безлічі різних команд пульта застосовується кодування переданих даних. Зараз переважно використовують наступні дві схеми кодування переданих даних:

Перша в пультах дистанційного керування стала застосовуватися фірмою Philips (протоколи RC4 і RC5, т. Н. Манчестерське кодування): Передача 0 доповнювалася одиницею, а передача 1 - нулем. Тобто 001 передається як 01 01 10. Відповідно посилка зчитується послідовно, і в ефір подається модульований сигнал тільки коли зустрічається одиниця.

Авторство другої схеми кодування приписується фірмі Sony. Спочатку завжди передається «1» модульованим сигналом, потім «0» - пауза. Тимчасової розмір одиниці завжди однаковий, а тимчасової розмір 0 - це кодовані дані, що передаються.

Довга пауза – передача одиниці, коротка пауза – передача нуля. Перед посилкою кодованих даних пульт завжди посиляє одне або кілька синхроповідомлень для того, щоб фотоприймач налаштував приймальний ланцюг (синхронізуватися з пультом по чутливості і фазі).

1.4 Антени

Задля збільшення робочої відстані у приладах з використанням технології Wi-Fi доцільно використовувати антени, вони використовуються для посилення сигналу від Wi-Fi обладнання. Застосування антен дозволяє зменшити вплив широкосмугових перешкод і збільшити зону покриття безпроводної мережі, що забезпечує стабільну та надійну роботу каналу зв'язку, також збільшує швидкість передачі даних.

Основними характеристиками і параметрами, які описують властивості Wi-Fi антен є: поляризація, вхідний імпеданс, смуга пропускання, коефіцієнт корисної дії (ККД), коефіцієнт підсилення антени (КП), діаграма направленості (ДН), коефіцієнт спрямованої дії (КСД), коефіцієнт стоячої хвилі (КСХ), еквівалентна ізотропно-випромінювана потужність (ЕІВП), фазову діаграму (ФД), шумова температура антени (ТА).

В залежності від діаграми спрямованості, умовно антени поділяють на три

типи: напрямлені, секторні і всенаправлені (кругові та штирьові). Антени також поділяються за місцем призначення їх використання на кімнатні та зовнішні. Зовнішні антени, як правило, більш потужні та мають захист від потрапляння бруду й вологи.

Задля збільшення робочої відстані в певному напрямку слід використовувати напрямлені антени, що поширюють сигнал не навколо себе, а в визначений бік.

Також слід обирати антену з найбільшим коефіцієнтом підсилення.

Найбільш поширені Wi-Fi антени – це півхвильові диполі (довжина півхвильового диполя має бути половиною довжини хвилі, він складається з двох половин, кожна з яких має четверту частину довжини хвилі)



Рисунок. 1.3 – Wi-Fi антена

1.5 Ретранслятори

Також задля збільшення робочої відстані пристрої, що використовують зв'язок по технології Wi-Fi, можливо використовувати ретранслятори. Вони отримують сигнал від передавального пристрою та поширюють його далі, таких ретрансляторів у лінії може бути декілька. Використання репітерів є доцільним, коли виникає потреба збільшити площу покриття безпроводної мережі, але не є можливим збільшувати потужність передавача. Каскад ретрансляторів в лінії передачі даних може збільшити дистанцію до кінцевого приладу в рази.

1.6. Безпроводові мережі

Безпроводні технології – підклас інформаційних технологій, які слугують для передачі інформації між двома або більше точками на відстані, без застосування провідного зв'язку [14]. Для передачі інформації можуть використовуватися радіохвилі, інфрачервоне, оптичне або лазерне випромінювання. Існують багато безпроводних технологій, найбільш відомими є Wi-Fi, WiMax, Bluetooth.

Безпроводні технології класифікують:

- По дальності дії (рис. 1.4):
 1. Безпроводні персональні мережі, до 10 метрів (WPAN);
 2. Безпроводні локальні мережі, до 100 метрів (WLAN);
 3. Безпроводні мережі масштабу міста, до 50 кілометрів (WMAN);
 4. Безпроводні глобальні мережі (WWAN)

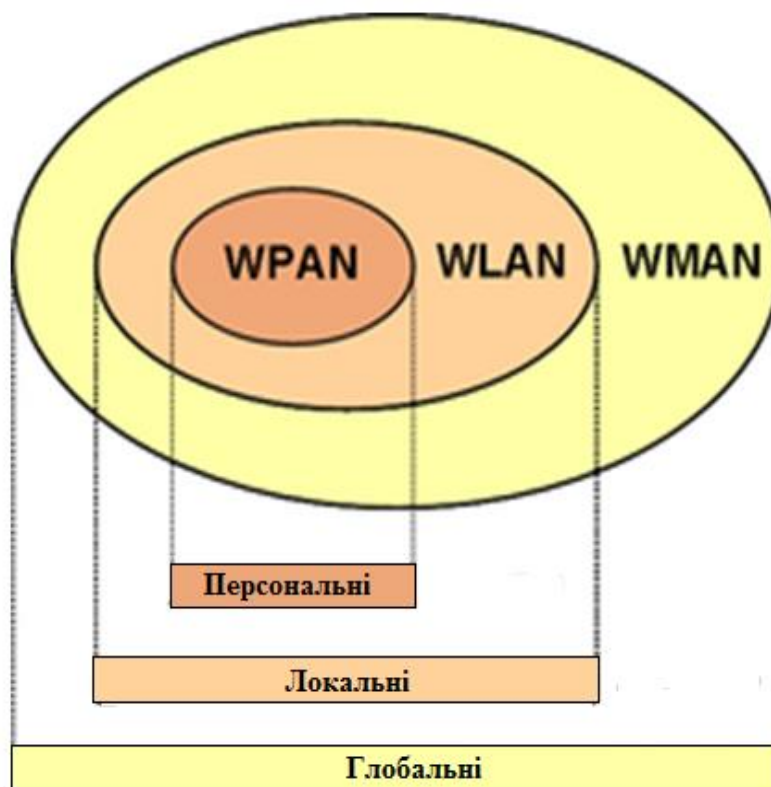


Рисунок 1.4 – Класифікація по дальності дії

- По топології:
 1. «Точка-точка»;
 2. «Точка-багатоточка»;
- По області призначення:
 1. Корпоративні безпроводні мережі;
 2. Безпроводні мережі операторів.

Також способом класифікації може слугувати одночасна характеристика максимальної швидкості передачі даних та максимальна відстань дії.

1.6.1. Технологія безпроводної передачі даних Bluetooth

Технологія Bluetooth (стандарт IEEE 802.15) стала першою технологією, що дозволяє організувати персональну мережу передачі даних (WPAN). Вона дозволяє виконувати передачу даних та голосу по радіоканалу на невеликі відстані (10-100 м) в діапазоні частот 2,4 ГГц, з'єднувати комп'ютери, мобільні телефони та інші пристрої при відсутності прямої видимості. [11]

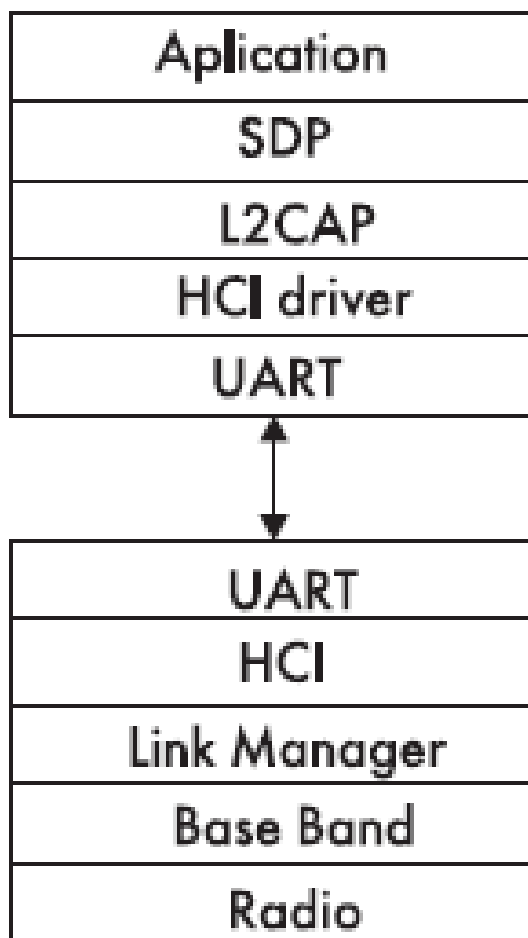


Рисунок 1.5 – Стек протоколу Bluetooth

Технологія BlueTooth підтримує як з'єднання «точка-точка», так і «точка-багатоточка». Два або більше пристроїв, що використовують один канал, утворюють пікомережу. Один пристрій працює як головний (master), а інші як підлеглі (slave). В одній пікомережі може бути до 7 активних підлеглих пристроїв. Взаємодіючі пікомережі утворюють розподілену мережу.

В кожній пікомережі діє тільки один головний пристрій, але підлеглі пристрої можуть входити в інші пікомережі. Окрім того, головний пристрій однієї пікомережі може бути підлеглим в іншій (Рис.1.5).

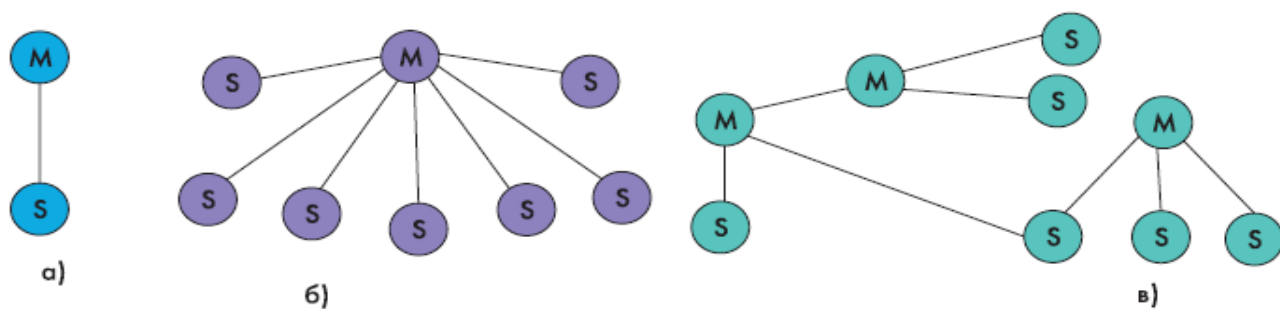


Рисунок 1.6 – Пікомережа з підлеглими пристроями.

а) з одним підлеглим пристроєм;

б) з декількома підлеглими пристроями;

в) розподілена мережа.

На зміну специфікації Bluetooth версії 1.1 була прийнята специфікація версії 1.2, до основних відмінностей якої відносять:

- Реалізацію технології адаптивної перебудови частоти каналу (AFH);
- Покращення голосового з'єднання;
- Зменшення часу для встановлення з'єднання між двома модулями Bluetooth.

Відомо, що Bluetooth та Wi-Fi використовують один діапазон частот 2,4 ГГц. Тому в випадках, коли Bluetooth пристрої знаходяться в зоні дії пристроїв Wi-Fi та виконують обмін даними між собою, можлива поява колізій та негативний вплив на працездатність пристроїв. Технологія AFH дозволяє уникнути появу колізій: під час обміну інформацією використовується стрибкоподібна перебудова частоти каналу, при виборі якого не враховуються частотні канали, на яких виконується обмін даними пристроїв Wi-Fi. Принцип дії технології AFH проілюстровано на рисунку 1.7.

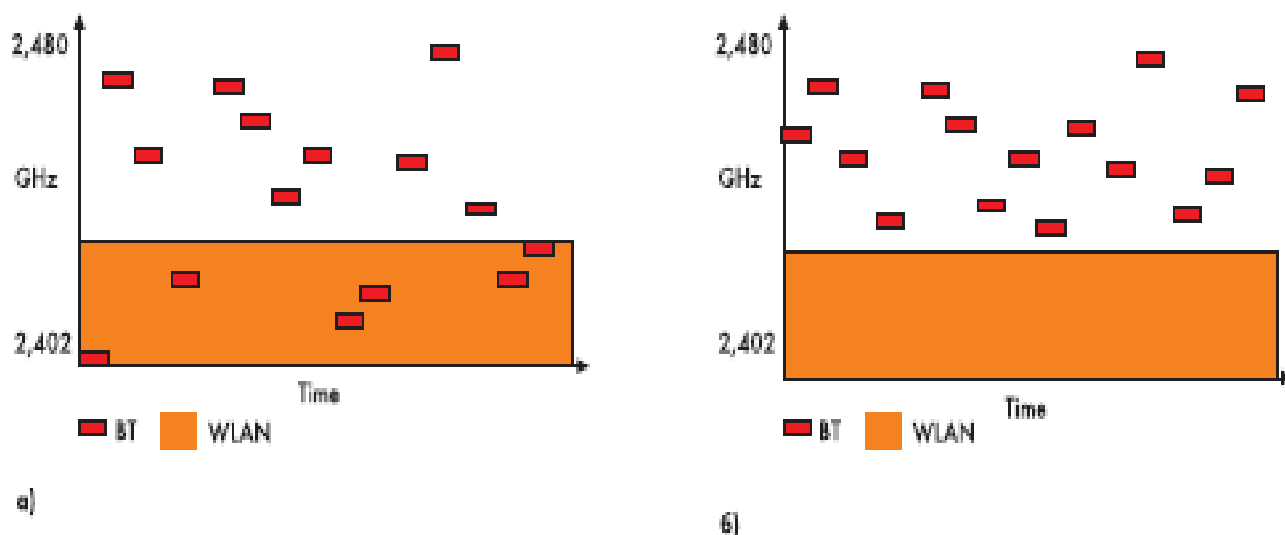


Рисунок 1.7 – Принцип дії технології AFH

а) колізії;

б) відхід від колізій за допомогою
адаптивної перебудови частоти каналу

Специфікація Bluetooth версії 2.0 підтримує технологію розширеної передачі даних (EDR). Вона дозволяє виконувати обмін даними на швидкості до 3 Мбіт/с, радіус дії складає приблизно 10 м, при відсутності прямої видимості, а при наявності – до 30 м.

Наразі розроблена та використовується версія Bluetooth 5.0. В цій версії набагато зменшене енергоспоживання, в порівнянні з минулими версіями, є можливість одночасного відтворення аудіо на двох пристроях. Можлива швидкість передачі даних до 2 Мбіт/с, максимальна робоча відстань – 240 м.

1.6.2. Технологія безпроводної передачі даних Wi-Fi

Wi-Fi – технологія безпроводної локальної мережі з пристроями на основі стандартів IEEE 802.11. Стандарт IEEE 802.11 є базовим стандартом для побудови безпроводних локальних мереж [14]. В теперішній час Wi-Fi сумісним є обладнання, що побудоване на стандарті IEEE 802.11a, b та g, також можливо з 802.11i, для забезпечення захищеного з'єднання. Wi-Fi працює в діапазоні 2,4 ГГц або 5 ГГц.

Початкова специфікація стандарту IEEE 802.11 встановлювала передачу даних на швидкості 1 та 2 Мбіт/с в неліцензійованому діапазоні частот 2,4 ГГц, а також спосіб управління доступом до фізичного середовища, який використовує метод множинного досупу з розпізнаванням носійної та з усуненням колізій – CSMA-CA. Для оцінки стану каналу, вільний чи зайнятий, використовується алгоритм оцінки рівня сигналу в каналі, за яким виконується вимірювання потужності сигналів на вході приймача та якість сигналу. Якщо потужність прийнятих сигналів на вході приймача нижче порогового значення, то канал вважається вільним, якщо їх потужність вище – вважається зайнятим.

Перше доповнення стандарту – IEEE 802.11b, що стало першим стандартом побудови безпроводних локальних мереж, зазнавши широкого розповсюдження. Максимальна швидкість передачі даних в ньому складає 11 Мбіт/с (реальна швидкість – до 7,1 Мбіт/с), така швидкість була досягнута за рахунок впровадження кодування послідовністю додаткових кодів (ССК). Для управління доступом до радіоканалу, також як і в початковому варіанті стандарту, використовується метод CSMA-CA та ортогональна частотна модуляція.

Наступним стандартом є IEEE 802.11a. Основна відмінність від початкової специфікації полягає в:

- Передача даних виконується в діапазоні частот 5 ГГц;
- Використовується ортогональна частотна модуляція;
- Максимальна швидкість передачі даних складає 54 Мбіт/с (реальна швидкість – 20 Мбіт/с).

Використання діапазону частот 5 ГГц при розробці специфікації 802.11a обумовлено насамперед тим, що даний діапазон менш завантажений, ніж діапазон 2,4 ГГц. Але, через використання цього діапазону, забезпечує надійну роботу обладнання при прямій видимості. Через це, при побудові мережі, виникає необхідність встановлення великої кількості точок доступу, що значно підвищує витрати.

В 2003 році була прийнята специфікація IEEE 802.11g, що встановлює

передачу даних в діапазоні 2,4 ГГц зі швидкістю до 54 Мбіт/с (реальна швидкість – приблизно 24,7 Мбіт/с). Для управління доступом до радіоканалу використовується метод CSMA-CA, а також ортогональна частотна модуляція (OFDM).

1.6.3. Технологія безпроводної передачі даних ZigBee

Технологія безпроводної передачі даних ZigBee, яку вважають за стандарт IEEE 802.15.4, з'явилася після Bluetooth та Wi-Fi. Її поява обумовлена необхідністю низького енергоспоживання та низької вартості для деяких систем дистанційного керування, висока швидкість передачі даних в цих випадках не була потрібна. ZigBee використовує діапазон частот 2,4 ГГц, 868 МГц та 915 МГц.

Мережевий рівень відповідає за знаходження пристроїв та конфігурацію мережі, підтримує 3 варіанти топології мережі (Рис. 1.8).

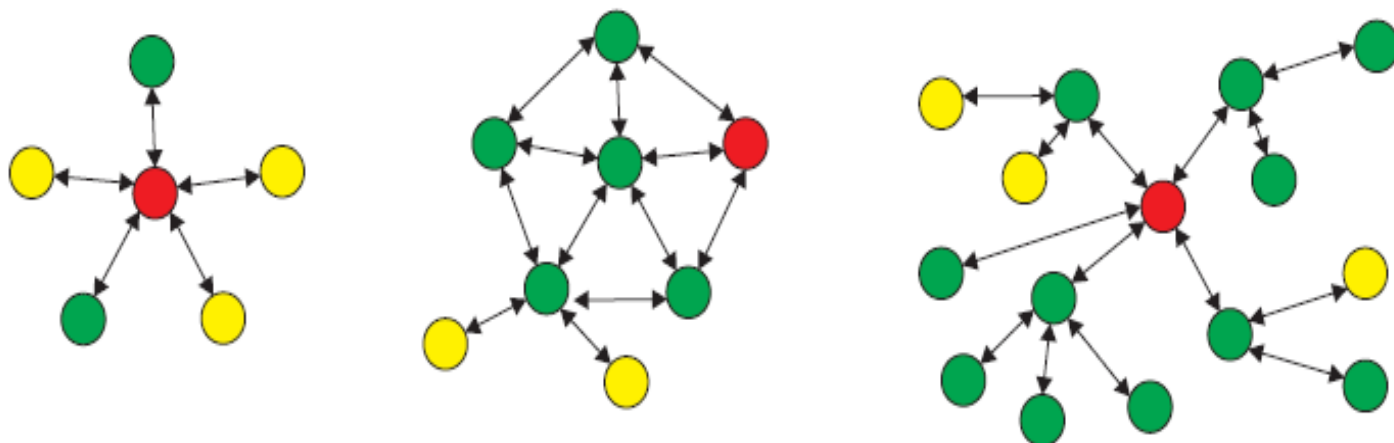


Рисунок 1.8 – Три варіанти топології мережі

- – Координатор персональної мережі;
- – Повністю функціональний пристрій;
- – Пристрій з обмеженим набором функцій.

Для забезпечення низької вартості інтеграції безпроводної технології передачі даних ZigBee, фізична реалізація апаратної частини стандарту

виконується в 2 варіантах: пристрої з обмеженим набором функцій (RFD) та повністю функціональні пристрої (FFD). Задля реалізації одної з топологій, приведених на рисунку 1.8, необхідна наявність хоча б одного FFD-пристрою, що виконує роль мережевого координатора.

Окрім поділу пристроїв на RFD та FFD, визначені три типи логічних пристроїв: координатор (узгоджуючий пристрій), маршрутизатор та кінцевий пристрій. Координатор виконує ініціалізацію мережі, контролює вузли, зберігає інформацію про налаштування кожного вузла, що підключений до мережі. Маршрутизатор відповідає за маршрутизацію повідомлень, що передаються по мережі від одного вузла до іншого. Кінцевий пристрій є будь-яким кінцевим пристроєм, підключеним до мережі.

Підключення та відключення кінцевого пристрою до мережі тільки в необхідні для взаємодії моменти дозволяє значно зменшити енергоспоживання.

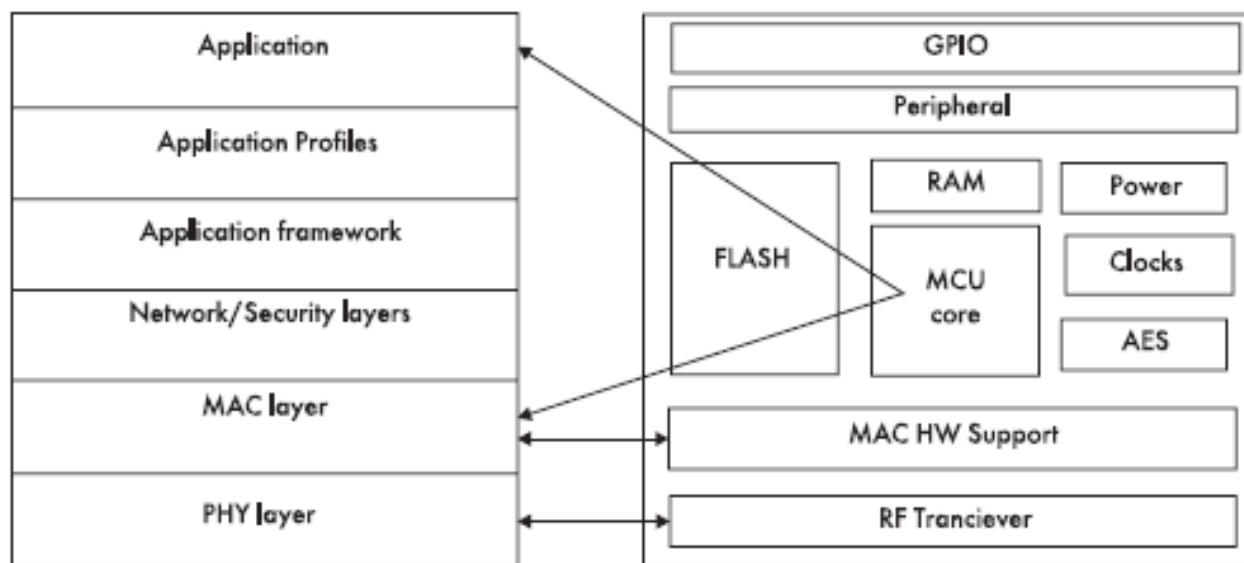


Рисунок 1.9 – Концепція виконання апаратної частини технології ZigBee

1.7. Wi-Fi модулі

1.7.1 Мікроконтролер ESP-8266

ESP-8266 — мікроконтролер китайського виробника Espressif з інтерфейсом Wi-Fi. Особливістю є відсутність флеш-пам'яті в SoC, програми користувача виконуються з зовнішньої флеш-пам'яті з інтерфейсом SPI (рис 1.10).

Програмні засоби розробки включають в себе:

- Компілятор. Він має відкриті вихідні коди;
- Бібліотеки для роботи з периферією мікроконтролера, протоколів Wi-Fi, TCP/IP;
- Засоби завантаження виконавчого файлу в пам'ять програм;
- Опціональну IDE.

Espressif вільно розповсюджує свій комплект засобів розробника. ESP-8266 має можливість оновлення програмного забезпечення через Wi-Fi.

Типове використання ESP-8266 як апаратної основи інтернету речей зазвичай має на увазі встановлення в будинках чи офісах. При цьому підключення до локальної мережі виконується з виходом в інтернет через роутер. Користувач пристрою може його контролювати з телефону, планшету чи комп'ютера через локальну мережу чи віддалено через інтернет.

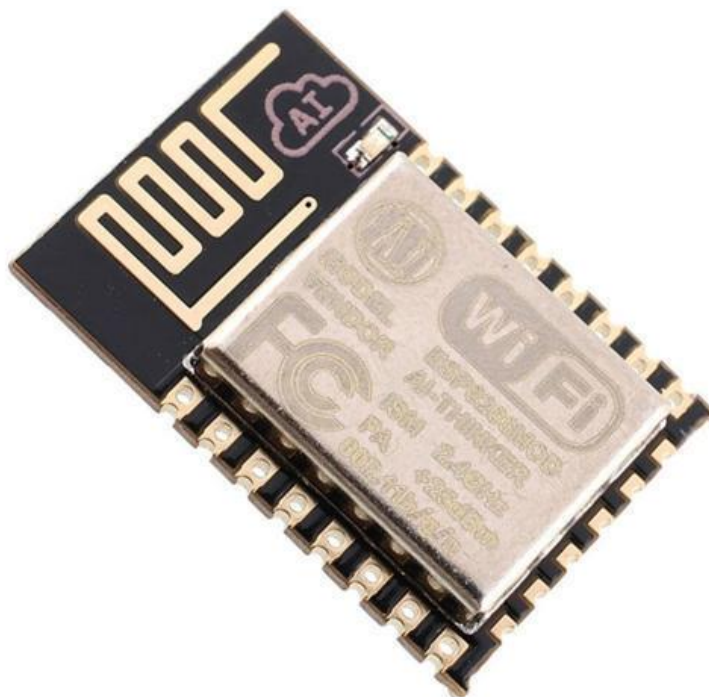


Рисунок 1.10 – Мікроконтролер ESP-8266

ESP-8266 може працювати як сервер так і клієнт. При нормальній роботі в локальній мережі ESP-8266 обирає конфігурацію кінцевого приладу. Для цього пристрою необхідно задати SSID Wi-Fi мережі, та, в закритих мережах, пароль. Для початкової конфігурації цих параметрів зручніший режим точки доступу. В режимі точки доступу пристрій відображається при стандартному пошуку мереж в смартфонах, планшетах чи комп'ютерах. Після підключення до пристрою потрібно відкрити HTML сторінку та задати мережеві параметри. Після чого пристрій підключиться до мережі в якості кінцевого приладу.

Після підключення до мережі, пристрій має отримати IP-параметри локальної мережі. Ці параметри можна задати вручну з параметрами Wi-Fi, або активувати сервіси автоматичної конфігурації. Після настройки IP-параметрів запит до сервера пристрою в локальній мережі зазвичай виконується по його IP-адресі, мережевому імені чи сервісу.

Часто потрібен доступ до приладу з інтернету. Наприклад, користувач із смартфона хоче перевірити стан підключених приладів, тощо. В цьому випадку

пристрій працює в режимі сервера, до якого звертається зовнішній клієнт.

1.7.2 Модуль WizFi220

WizFi220 – Wi-Fi модуль корейського виробництва, фірми WizNet (рис. 1.11).

Характеристики:

- Розміри: 32*24,5 мм;
- Час старту – 20 мс;
- Споживання струму в режимі очікування – 34 мкА;
- Споживання струму в режимі прийому – 125 мА;
- Споживання струму в режимі передачі – 250 мА;
- Підтримує стандарти 802.11 b/g/n;
- Підтримує шифрування WEP, WPA/WPA2-PSK;
- Напруга живлення – 3,3 В.

Модуль WizFi220 може працювати як сервер так і клієнт. Контролюється за допомогою АТ-команд.

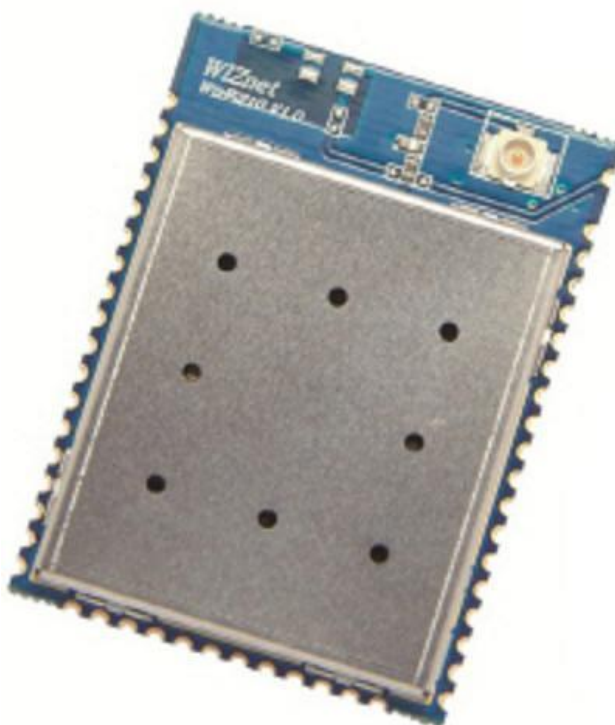


Рисунок 1.11 – Wi-Fi модуль WizFi220

1.7. 3 Модуль CC3000

CC3000 – Wi-Fi модуль виробництва фірми Texas Instruments (рис. 1.12). Модуль побудований на базі Wi-Fi рішень шостого покоління. CC3000 позиціонується виробником як закінчене апаратно-програмне рішення з вбудованими мережевими протоколами, дозволяюче додати безпроводний Wi-Fi доступ навіть в мікроконтролер з низькою потужністю.

Характеристики:

- Підтримує стандарти 802.11 b/g/;
- Підтримує шифрування WEP, WPA/WPA2;
- Робоча частота – 2,4 ГГц;
- Напруга живлення – 2,7 – 4,8 В;
- Споживання струму в режимі очікування – 5 мкА;
- Споживання струму в режимі прийому – 92 мА;

- Час старту – 700 мс;
- Розміри: 16,3*13,5*2мм.

Модуль C3000 може працювати як сервер так і клієнт. Програмується на мові С.

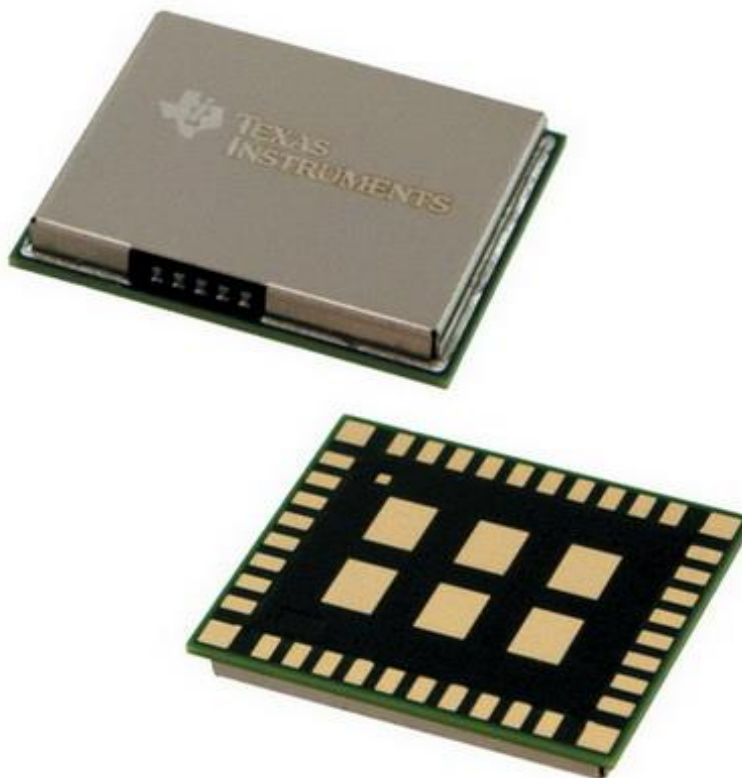


Рисунок 1.12 – Wi-Fi модуль C3000

Модуль включає в себе контролюємий стабілізатор для вбудованого процесора та може працювати від мережевого джерела живлення чи від батарей. Модуль C3000 виступає в ролі підлеглого пристрою.

Модуль має якісну та зрозумілу документацію, підтримується великим набором засобів розробки ТІ. Для тестування підходять прості плати серії Launchpad на базі мікроконтролерів серії MSP та багатофункціональні засоби розробки на базі процесорів серії MSP, TM, LM. Для роботи з цими платами можна використовувати швидкоз'ємні оціночні модулі на роз'ємаї (мезонінові плати), які представляють собою невеликі перехідні плати з модулем C3000, антеною та мінімально необхідними елементами.

1.7. 4 Модулі серії RN та MRF

Компанія Microchip Technology Inc. виробляє декілька Wi-Fi модулів стандарту 802.11b та 802.11b/g з дуже низьким споживанням. Модулі мають невеликі розміри та великий функціонал.

Компанія MTI пропонує два сімейства модулів: серії RNxxx (рис. 1.13) та MRFxxx (рис. 1.14). Головна відмінність модулів полягає в розташуванні TCP/IP стека по відношенні до модуля. Модулі RNxxx мають вбудований процесор з TCP/IP стеком, а для модулів MRFxxx потрібен стек в зовнішньому мікроконтролері.



Рисунок 1.13 – Wi-Fi модуль RN



Рисунок 1.14 – Wi-Fi модуль MRF

Для підтримки розробок компанія Microchip надає безкоштовний стек протоколів TCP/IP в вихідних кодах для 16 та 32-розрядних PIC мікроконтролерів.

Управління модулями RN базується на ідеї управлінні апаратурою за допомогою AT команд. Модулі працюють в двох режимах: режимі даних та режимі управління.

Модулі RN відповідають стандарту 802.11 b/g та являють собою закінчене сумісне рішення за низьким споживанням струму. В активному режимі споживання струму – 35 мА, в режимі енергозберігання – 4 мкА.

Можливість передачі даних та повернення в енергозберігаючий режим за час менше 100 мілісекунд дозволяють цим модулям працювати довгий час від одного комплекту батарей.

Модулі Microchip підтримують WEP, WPA1 та WPA2 режими шифрування, також підтримують Enterprise. Підтримують налаштування та встановлення з'єднання через WPS, CLI та web-інтерфейс. Містять конфігураційний web-сервер, що надає змогу під'єднатися до створеної мережі на налаштовувати модуль через браузер. В режимі сервера можна задати мережевий режим: клієнт (під'єднання до мережі) або сервер (точка доступу), просканувати мережі та

вибрати до якої з них підключитись, задати тип мережі (відкрита чи закрита), ключ доступу та ім'я мережі.

Модулі мають вбудований HTML клієнт, за допомогою якого можна отримувати чи відправляти дані на сервер.

1.7.5 Модуль WGM110

Модуль реалізує стандарт IEEE 802.11 b/g/n. Може працювати як клієнт або точка доступу, забезпечуючи підключення до 5 клієнтів. Висока поужність передавача дозволяє передавати дані до 450 метрів, за умови прямої видимості.

WGM110 (рис. 1.15) може використовуватися з будь-яким зовнішнім мікроконтролером, має інтерфейси USB, UART, SPI. Модуль має вбудований 32-бітний мікроконтролер ARM Cortex-M3 з можливістю завантаження програми користувача. Модуль виробляється з вбудованою чіп-антеною або з роз'ємом для підключення зовнішньої антени. Підтримує роботу в режимі клієнт а та сервера.



Рисунок 1.15 – Wi-Fi модуль WGM110

Характеристики:

- Живлення: 2,7-4,8 В;
- Розміри: 21*14,4*2 мм;
- Споживання струму в режимі передачі – 261 мА;
- Споживання струму в режимі прийому – 81 мА;
- Споживання струму в режимі енергозберігання – 120 мкА.

За необхідності розробки програмного забезпечення слід використовувати Simplicity Studio та набір Wizard Gecko Wi-Fi SDK, що доступні для завантаження на сайті виробника, також наявні готові варіанти, що вирішують основні задачі.

1.7.6 Модуль AMW007

Модуль реалізує стандарт IEEE 802.11 b/g/n. Підтримує режим сервера та клієнта. Модуль AMW007 (рис. 1.16) має 2 Мб вбудованої флеш-пам'яті з доступною для користувача файловою системою. Підтримує різні режими енергоспоживання (режим енергозберігання, режим глибокого сну). Має інтерфейси USB, UART.



Рисунок 1.16 – Wi-Fi модуль AMW007

Характеристики:

- Живлення: 3-3,6 В;
- Розміри: 12*11*1,8 мм;
- Споживання струму в режимі передачі – 200 мА;
- Споживання струму в режимі прийому – 65 мА;
- Споживання струму в режимі енергозберігання – 31 мкА.

1.7.7 Модуль WF121

Модуль WF121 (рис. 1.17) реалізує стандарт IEEE 802.11b/g/n. Може працювати як клієнт та точка доступу. Відрізняється високою потужністю передавача та чутливістю приймача, завдяки чому забезпечує передачу даних на відстань до 500 м. Має вбудований стек TCP/IP і може використовуватись з будь-яким зовнішнім мікроконтролером. Для обміну даними з хост-процесором призначені інтерфейси UART, SPI та USB. Модуль має вбудований 32-бітний мікроконтролер Microchip PIC32MX695F512H з можливістю завантаження користувацької програми. Модуль поставляється з U.FL роз'ємом для підключення зовнішньої антени або з вбудованою антеною.



Рисунок 1.17 – Wi-Fi модуль WF121

Характеристики:

- Живлення: 2,3-3,6 В;
- Розміри: 26,2*15,4*2,1 мм;
- Споживання струму в режимі передачі – 143 мА;
- Споживання струму в режимі прийому – 127 мА;
- Споживання струму в режимі енергозберігання – 226 мкА.

Взаємодія з Wi-Fi модулем відбувається за допомогою двійкового протоколу BGAPI по інтерфейсу UART. Можливо використовувати бібліотеки BGLIP.

Висновки

Засоби для знешкодження вибухонебезпечних предметів з дистанційним керуванням складаються з командно-передавального пристрою та приймально-виконачого, також в лінії зв'язку може бути повторювач. В даному випадку в пристрої використовується Wi-Fi, командно-передавальним пристроєм слугує смартфон, планшет чи ноутбук.

Приймально-виконавчий пристрій складається з Wi-Fi модуля, мікроконтролера, набору реле та антени.

Задля більш безпечного використання, доцільно використовувати додаткові антени та повторювачі у лінії зв'язку.

2. ШЛЯХИ ВДОСКОНАЛЕННЯ ЗАСОБІВ ДЛЯ ЗНЕШКОДЖЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

2.1. Особливості засобів розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів

В наш час широко розповсюджені військові конфлікти, тому наразі тема розробки технічних заходів, що спрямовані на подолання наслідків проведення бойових дій, є актуальною. Першочерговою задачею є знешкодження не спрацювавших боєприпасів на територіях з цивільним населенням. Задля безпеки саперів використовуються пристрої з дистанційним керуванням. Такі пристрої надають більшу надійність та безпечність, порівняно з вогнепроводними шнурами та часовими механізмами. Пристрої дистанційного підриву дають змогу знешкоджувати вибухонебезпечні предмети на великих відстанях. З розвитком сучасних технологій є не раціональним використання застарілих підривних машинок, що є дуже габаритними, натомість кращим варіантом є використання малогабаритних мікроконтролерних збірок з застосуванням безпроводових технологій, наприклад Wi-Fi.

Використання Wi-Fi є зручним, бо можливо керувати пристроєм з смартфона чи планшета, пристрій не потребує спеціального пульта управління.

Аби зрозуміти, чи необхідно розробляти та покращувати нові засоби для знешкодження вибухонебезпечних предметів з керуванням по Wi-Fi, необхідно провести аналіз уже існуючих розробок на ринку, визначити їх вартість та функціональність. Метою аналізу є виявлення переваг та недоліків в уже існуючих системах.

Так як пристрій є поєднанням системи керування через канал Wi-Fi та вибухової машинки, а аналогічну систему знайти не вдалося, то розглянемо окремо кожен тип пристроїв.

Конденсаторна підривна машинка КПМ-6

Характеристики КВМ-6 (рис.2.1):

- Напруга на індукторі (при 4 об./хв.) ~ 100 В;
- Ємність конденсаторної батареї - 940 мкФ;
- Енергія конденсаторної батареї - 17,8 Дж;
- Напруга на конденсаторній батареї - 190...200 В;
- Напруга спрацювання сигнальної лампи - 195 В;
- Приблизна вартість: ≈ 500 грн.

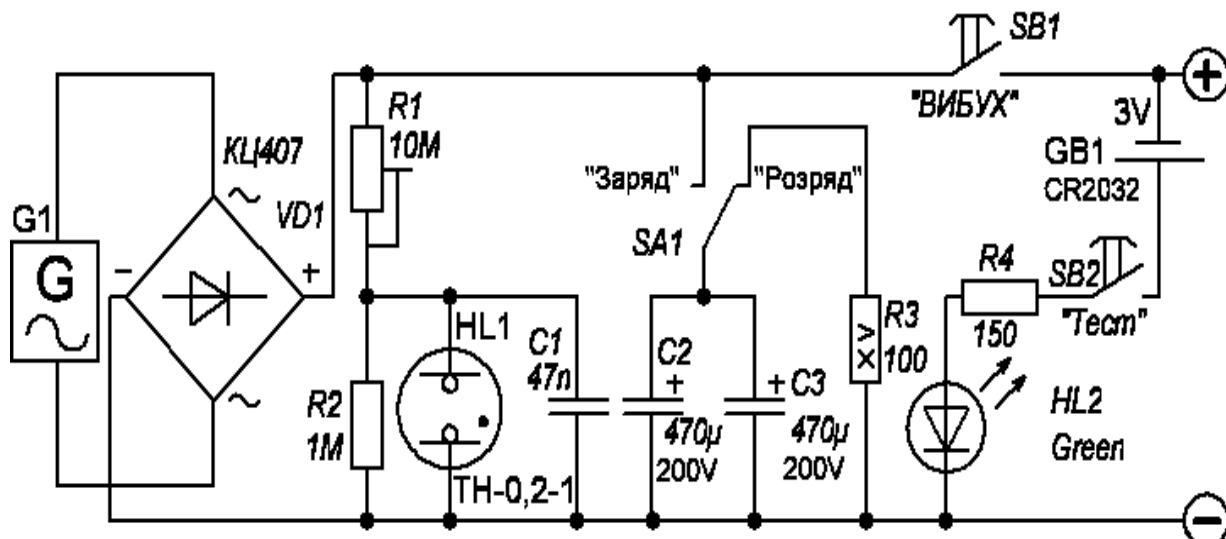


Рисунок 2.1 – Конденсаторна підривна машинка КПМ-6

Даний пристрій має можливість під'єднання великої кількості електродетонаторів, високу надійність та дальність дії, яка залежить лише від довжини провідника.

До недоліків слід віднести великі розміри пристрою та необхідність користуватися довгим провідником.

Конденсаторний вибуховий пристрій КВП-1/100М

Характеристики КВП-1/100М (рис.2.2):

- Первинне джерело струму - 3 сухих елементи типу «373»;
- Ємність конденсатора-накопичувача - 10 мкФ;
 - Напруга на конденсаторі-накопичувачі - 600 В;
 - Кількість ЕД в мережі при послідовному з'єднанні – 100;

- Максимальний опір послідовної мережі - 320 Ом;
- Час зарядки конденсатора-накопичувача - до 8 с;
- Число робочих циклів – 2500;
- Час подачі імпульсу струму - 2-4 мс;
- Вага приладу - 2 кг;
- Приблизна вартість: ≈ 600 грн.

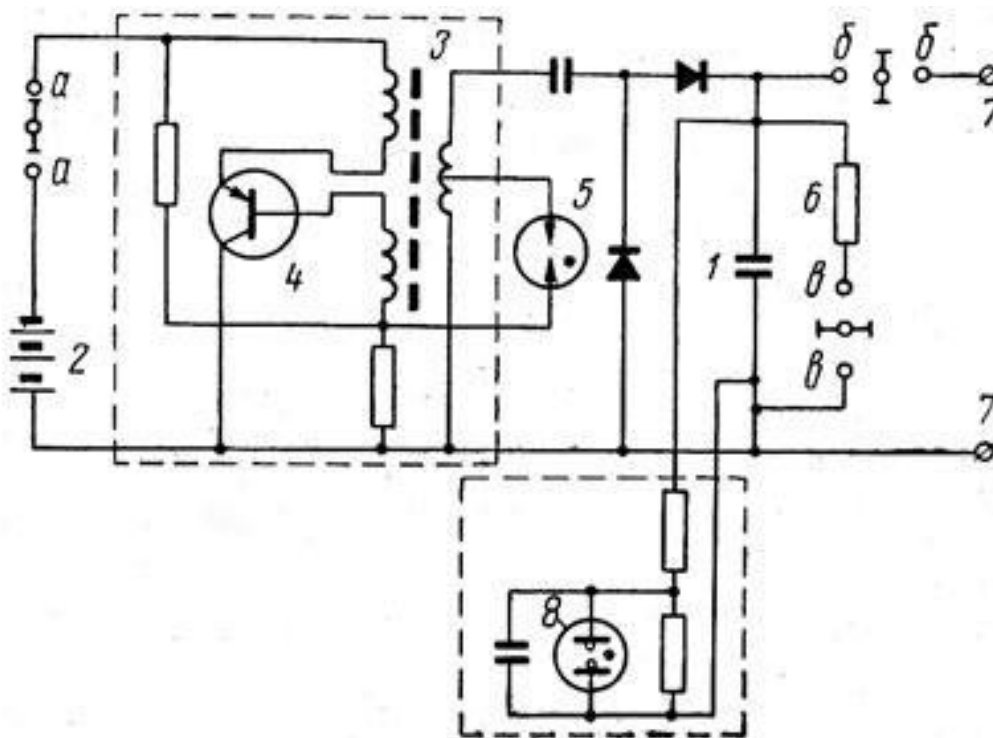


Рисунок 2.2 – Конденсаторний вибуховий пристрій КВП-1/100М

Даний пристрій має можливість під'єднання досить великої кількості електродетонаторів, високу надійність та габарити менші ніж у КПМ, досить зручний у використанні.

До недоліків слід віднести габарити та вагу пристрою, відсутність керування безпроводовим способом.

Піротехнічний пульти ПП-16

Характеристики ПП-16 (рис. 2.3):

- Зовнішнє живлення 12 В;

- 16 каналів;
- Час подачі імпульсу – 2 мс;
- Сила струму 7-10 А;
- Вага приладу – 0,7 кг;
- Можливість підключення Wi-Fi модуля;
- Приблизна вартість: ≈ 7000 грн.



Рисунок 2.3 – Піротехнічний пульт ПП-16

Даний пристрій має можливість під'єднання досить великої кількості електродетонаторів, високу надійність та габарити менші ніж у КПМ та КВП-1, досить зручний у використанні, також має можливість підключення Wi-Fi модуля.

До недоліків слід віднести вагу пристрою, габарити та високу вартість.

Піротехнічний пульт Pyro-RF

Характеристики Pyro-RF (рис. 2.4):

Приймач:

- Живлення – 12 В;
- Споживання струму в режимі очікування до 0,02 А;

- Споживання струму в режимі тестування до 0,06 А;
- Кількість каналів 10 шт;
- Сила струму 1,2 А;
- Габарити 120*95*30 мм;
- Вага – 0,18 кг;

Передавач:

- Живлення – 9 В;
- Споживання струму при передачі до 0,04 А;
- Споживання струму в режимі очікування до 0,01 А;
- Кількість каналів – 12 шт ;
- Розміри 200*60*25 мм ;
- Вага – 0,2 Кг;
- Приблизна вартість: \approx 5500 грн.



Рисунок 2.4 – Піротехнічний пульт Pyro-RF

Даний пристрій має можливість під'єднання досить великої кількості електродетонаторів, високу надійність, досить зручний у використанні, також контролюється безпроводово.

До недоліків слід віднести високу вартість та відсутність керування з смартфона чи планшета.

2.2. Визначення параметрів засобів для знешкодження вибухонебезпечних предметів, що можливо покращити

Задля визначення шляхів вдосконалення засобу для знешкодження вибухонебезпечних предметів з керуванням через Wi-Fi, слід встановити параметри, які можливо та слід покращити. В пристроях для знешкодження вибухонебезпечних предметів з дистанційним керуванням важливими параметрами є надійність, радіус дії, габарити, вартість та кількість електродетонаторів, що можливо підключити. Не всі параметри можуть бути одночасно впроваджені, щоб обрати важливіші, слід визначити їх відносну важливість.

2.2.1. Визначення відносної важливості основних параметрів

Для використання у цілях знешкодження вибухонебезпечних предметів, даний пристрій має бути безвідмовним, щоб виключити можливість несвоєчасного спрацювання чи спрацювання не усіх під'єднаних елементів, має бути невеликих розмірів та ваги, задля зручності транспортування та можливості постійної наявності достатньої кількості пристроїв в користувача в будь-якій ситуації без необхідності впровадження додаткових технічних заходів для транспортування, також прилад має бути низької вартості, адже, в певних випадках, пристрій втратить здатність до повторного використання та буде знищений разом з вибухонебезпечним предметом, кількість електродетонаторів, що можливо підключити, має бути якомога більшою, для можливості знешкодження одночасно великої кількості чи дуже габаритних вибухонебезпечних предметів. Для забезпечення безпеки користувачів цих засобів, робоча відстань має бути якомога більшою та має бути можливість її

змінювати за потреби, повинна бути можливість контролю пристрою поза зоною прямої видимості.

Оскільки безпека використання є головним фактором при роботі з вибухонебезпечними матеріалами, а зменшення вартості призводить до зменшення надійності, тому найбільш важливими параметрами пристрою, в даному випадку, є радіус дії та надійність.

Наступним етапом для визначення шляхів вдосконалення пристрою має бути визначення діапазону покращення основних параметрів, щоб розуміти максимальні можливості приладу, не втрачаючи актуальності впровадження вдосконалень.

2.2.2. Визначення діапазону покращення основних параметрів

Діапазон покращення основних параметрів залежить від можливостей замовників та розроблювачів, від впливу одних параметрів на інші, від потреб користувача та можливостей сучасних технічних засобів.

Радіус дії приладу залежить від потужності передавача, наявності антени та її коефіцієнту підсилення, наявності та кількості ретрансляторів у лінії зв'язку. Надійність залежить від якості матеріалів та технічних засобів, також якості збірки пристрою.

Зниження вартості можливе за рахунок використання недорогих матеріалів, але це призводить до зниження надійності, що є негативним фактором. Зменшення габаритів можливе при розміщенні елементів в два рівні, при цьому зменшується його міцність та надійність, але пристрій не має значних розмірів й при розміщенні в один рівень. Кількість електродетонаторів, що можливо під'єднати, залежить від кількості виходів мікроконтролера та потужності блоку живлення. Надійність пристрою можливо покращити за рахунок використання високоякісних перевірених матеріалів та технічних засобів, що збільшить вартість, але в порівнянні з аналогами вартість залишиться досить низькою. Радіус дії можливо збільшити в декілька разів, при використанні додаткової

антени та повторювачів в лінії зв'язку. Стандартна друкована антена, що використовується у мікроконтролерах з Wi-Fi модулем, забезпечує зв'язок на відстані до 350 метрів, використання зовнішньої антени збільшує відстань до 450 метрів, за використання репітера в лінії зв'язку радіус дії збільшується до двох разів.

Отже можливо підвищити надійність пристрою за рахунок якісним матеріалів, та збільшити радіус дії в рази, за рахунок використання повторювачів в лінії зв'язку. Надалі буде наводитись система з одним повторювачем, адже їх кількість може збільшуватись, не потребуючи складних дій.

2.2.3. Формування задач досліджень

Формування задач та мети досліджень є важливим етапом початку роботи над технічними рішеннями. Для впевненого досягнення запланованих покращень слід чітко визначити мету та задачі.

Задачами досліджень є:

- збільшення робочої відстані приладу;
- покращення надійності;
- визначення діапазону збільшення радіусу дії пристрою в разі встановлення антени та підключення повторювача у лінію зв'язку, збільшення надійності внаслідок використання якісних матеріалів.

Висновки

В ході проведення порівняльного аналізу було визначено, що прямих аналогів пристрою немає, але за них можуть слугувати деякі типи піротехнічних пультів.

Було визначено, що прилад можливо покращити, а саме – підвищити його надійність та збільшити радіус дії.

За умови досягнення встановленої мети досліджень, пристрій буде відповідати усім вимогам потенційних користувачів.

3. РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

3.1 Опис ідеї проекту

У розділі проаналізовано та подано у вигляді таблиць :

- зміст ідеї (що пропонується);
- можливі напрямки застосування;
- основні вигоди, що може отримати користувач товару (за кожним напрямком застосування);
- чим відрізняється від існуючих аналогів та замінників.

Таблиця 3.1 – Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигода користувача
Розробка засобів розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів	Знешкодження вибухонебезпечних предметів	Використання малогабаритного пристрою, яким можливо керувати з смартфона, планшета чи ноутбука
	Використання у піротехнічних заходах	Можливість зручного контролю запусків, побудови розвиненої піротехнічної мережі

Аналіз потенційних техніко-економічних переваг порівняно з пропозиціями конкурентів передбачає:

- визначення переліку техніко-економічних властивостей та характеристик;

- визначення попереднього кола конкурентів або товарів-замінників чи товарів-аналогів, що вже існують на ринку, та проведення збору інформації щодо значень техніко-економічних показників для ідеї власного проекту та проектів конкурентів;

- проведення порівняльного аналізу показників: для власної ідеї визначаються показники, що мають а) гірші значення (W, слабкі); б) аналогічні (N, нейтральні) значення; в) кращі значення (S, сильні) (табл. 3.2).

Таблиця 3.2 – Визначення характеристик ідеї проекту

№ п/п	Техніко-економічні характеристики ідеї	Мій проект	Конкурент 1	Конкурент 2	W	N	S
1	Економічні	500 грн	7000 грн	5500 грн	-	-	+
2	Призначення	Можливість збільшувати робочу відстань безпроводовим методом в разі за рахунок повторювачів	Можливість збільшення робочої відстані безпроводовим методом за рахунок підключення Wi-Fi модуля	Немає можливості збільшення робочої відстані безпроводовим методом	-	-	+
3	Надійності	Висока надійність	Висока надійність	Висока надійність	-	+	-
3	Технологічні	Працює після нескладних налаштувань	Працює після нескладних налаштувань	Працює після нескладних налаштувань	-	+	-
5	Ергономічні	Зручне при використанні	Зручне при використанні	Зручне при використанні	-	+	-
6	Органолеп.	-	-	-	-	+	-
7	Естетичні	Інтуїтивно зрозумілий зовнішній вигляд	Зручний та зрозумілий	Зручний та зрозумілий	-	+	-
8	Транспор-табл.	Декілька малогабарит-	Об'ємна упаковка	Декілька малогабарит-	-	-	+

№ п/ п	Техніко- економічні характери- стики ідеї	Мій проект	Конкурент 1	Конкурент 2	W	N	S
		них блоків		них блоків			
9	Екологічно сті	Помірно шкідливий при утилізації	Помірно шкідливий при утилізації	Помірно шкідливий при утилізації	-	+	-
10	Безпеки	Безпечно	Безпечно	Безпечно	-	+	-

Визначений перелік сильних, нейтральних та слабких характеристик і властивостей ідеї потенційного товару є підґрунтям для формування його конкурентоспроможності.

3.2 Технологічний аудит ідеї проекту

В межах даного підрозділу проведено аудит технології, за допомогою якої можна реалізувати ідею проекту. Визначення технологічної здійсненності ідеї проекту передбачає аналіз таких складових (табл. 3.4):

- за якою технологією буде виготовлено товар згідно ідеї проекту;
- чи існують такі технології чи їх потрібно розробити/допрацювати;
- чи доступні такі технології авторам проекту.

Таблиця 3.3 – Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології реалізації	Наявність технологій	Доступність технологій
1	Розробка засобів розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів	Мікроконтролери	Наявні	Доступно
		Модулі Wi-Fi	Наявні	Доступно
		Анени	Наявні	Доступно
		Програмне забезпечення виконавчого пристрою	Потребує розробки	Доступно
		Програмне	Потребує	Доступно

		забезпечення для передавального пристрою	розробки	
Обрана технологія ідеї проекту: Програмне забезпечення виконавчого пристрою				

3.3 Аналіз ринкових можливостей запуску стартап-проекту

Визначення ринкових можливостей та ринкових загроз, що впливають на ринкове впровадження проекту, дозволяє спланувати напрями розвитку проекту з урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій конкурентних проектів. Визначення загроз та можливостей в майбутньому буде впливати на конкурентоспроможність товару. Спочатку проводиться аналіз попиту: наявність попиту, обсяг, динаміка розвитку ринку (табл. 3. 4).

Таблиця 3. 4 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1.	Кількість головних гравців, од	2
2.	Загальний обсяг продаж, грн/ум.од	6250
3.	Динаміка ринку (якісна оцінка)	Зростає
3.	Наявність обмежень для входу (вказати характер обмежень)	Немає
5.	Специфічні вимоги до стандартизації та сертифікації	Немає
6.	Середня норма рентабельності в галузі або по ринку, %	100%

Середня норма рентабельності в галузі (або по ринку) порівнюється із банківським відсотком на вкладення. За результатами попереднього оцінювання ринок є привабливим для входження, тому актуальність товару не втрачається.

Надалі визначаються потенційні групи клієнтів, їх характеристики, та формується орієнтовний перелік вимог до товару для кожної групи, за потребами користувачів, що дає змогу чіткіше визначити план впровадження товару на ринок (табл. 3.5).

Після визначення потенційних груп клієнтів має бути проведений аналіз ринкового середовища: складені таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому перешкоджають (табл. №№ 3.6, 3.7). Аналіз ринкового середовища надає змогу знайти слабкі та сильні сторони впроваджуваного товару в різних сферах його використання. Фактори в таблиці подані в порядку зменшення значущості.

Таблиця 3.5 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Знешкодження вибухонебезпечних предметів	Збройні сили, ДСНС.	Потреба в надійності, малих габаритах, низькій вартості.	Товар має забезпечувати високу надійність, безвідказність, бути зручним у транспортуванні.
2	Використання в піротехнічній справі	Піротехніки, цивільне населення	Потреба в зручності та зрозумілості використання.	Товар має забезпечувати простоту у використанні.

Таблиця 3.6 – Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1.	Потреба в технічному оснащенні та матеріалах	Продукт потребує специфічних матеріалів, обладнання та середовища тестування	Укладання договірних відносин з державними та комерційними структурами, задля фінансування

Таблиця 3.7 – Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
-------	--------	------------------	--------------------------

1.	Конкуренція	Спонукає розробляти і виробляти нові продукти, знижувати витрати їх виробництва і вартість	Збільшення функціональності та якості товару
2.	Попит	Існування стійкого попиту означає, що більшість клієнтів зацікавлені у введенні інновацій	Рекламна діяльність, демонстрація товару на тематичних заходах

Надалі проведений аналіз пропозиції: визначені загальні риси конкуренції на ринку (табл. 3.8)

Таблиця 3.8 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства
1. Вказати тип конкуренції олігополія	На ринку присутня невелика кількість фірм, що виробляють пристрої для знешкодження вибухонебезпечних предметів	Підвищувати якість товару та функціональність
2. За рівнем конкурентної боротьби національний	Місцезнаходження виробників не обмежується територіально; виробництва розташовані в різних містах	Створювати веб-сайт компанії
3. За галузевою ознакою внутрішньогалузева	Економічна боротьба між різними товаровиробниками, що діють в одній галузі економіки, виробляють і реалізують однакові товари, які задовольняють одну й ту саму потребу, але мають відмінності у виробничих затратах, якості, ціні, тощо	Відстежувати зміни в продукції конкурентів
4. Конкуренція за видами товарів: товарно-видова	Конкуренція між товарами одного виду	Покращувати якість, надійність та функціональність товару
5. За характером конкурентних переваг: цінова	Передбачає продаж продукції за більш низькими цінами, ніж конкуренти.	Продавати товар за низькою ціною.

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства
6. За інтенсивністю не марочна	Боротьба носить не марочний характер, бренд не має великого значення	Покращення характеристик товару

Після аналізу конкуренції проведений більш детальний аналіз умов конкуренції в галузі (за моделлю 5 сил М. Портера) (табл. 3.9).

Таблиця 3.9 – Аналіз конкуренції в галузі за М. Портером

	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари - замітники
Складові аналізу	"Pyro-RF" "Cobra" "Firing by Wire"	Немає	Виробники піропультів	Вимоги до якості (надійність, зручність користування, низька вартість, висока функціональність)	Замінників немає
Висновки	Інтенсивність досить висока	Немає	Є певна залежність від постачальників	Товар має бути якісним, зручним та дешевим	Обмежень немає

Щоб бути конкурентоспроможним на ринку, для розробки товару слід залучати кваліфікованих спеціалістів у галузі техніки та програмування.

На основі аналізу конкуренції, наведеного в табл. 3.9, а також із урахуванням характеристик ідеї проекту (табл. 3.2), вимог споживачів до товару (табл. 3.5) та факторів маркетингового середовища (табл. №№ 3.6- 3.7) визначається та обґрунтовується перелік факторів конкурентоспроможності. Аналіз оформлюється за табл. 3.10.

Таблиця 3.10 – Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування
1.	Ступінь задоволення потреб користувача	Продукт має бути малогабаритним та мати зрозумілий інтерфейс, щоб користувачі могли користуватись ним без складнощів в будь-яких умовах
2.	Якість розробки з точки зору оптимальності показників надійності	Продукт має працювати стабільно
3.	Наявність наукових ресурсів	Для створення високоякісного та стабільно працюючого обладнання потрібні інженери
4.	Економічний	Ціна на товар має бути не високою, щоб знайти потенційних заказників та покупців

За визначеними факторами конкурентоспроможності (табл. 3.10) проводиться аналіз сильних та слабких сторін стартап-проекту (табл. 3.11).

Таблиця 3.11 – Порівняльний аналіз сильних та слабких сторін проекту

№ п/п	Фактор конкурентоспроможності	Бали 1-20	-3	-2	-1	0	+1	+2	+3
1.	Ступінь задоволення потреб користувача	20	+						
2.	Якість розробки з точки зору оптимальності показників надійності	20					+		
3.	Наявність наукових ресурсів	15			+				
4.	Економічний	20	+						

Фінальним етапом ринкового аналізу можливостей впровадження проекту є складання SWOT-аналізу (матриці аналізу сильних (Strength) та слабких (Weak) сторін, загроз (Troubles) та можливостей (Opportunities) (табл. 3.12) на основі виділених ринкових загроз та можливостей, та сильних і слабких сторін (табл. 3.11).

Перелік ринкових загроз та ринкових можливостей складається на основі аналізу факторів загроз та факторів можливостей маркетингового середовища. Ринкові загрози та ринкові можливості є наслідками (прогнозованими результатами) впливу факторів, і, на відміну від них, ще не є реалізованими на ринку та мають певну ймовірність здійснення. Наприклад: зниження доходів потенційних споживачів – фактор загрози, на основі якого можна зробити прогноз щодо посилення значущості цінового фактору при виборі товару та відповідно, – цінової конкуренції (а це вже – ринкова загроза).

Таблиця 3.12 – SWOT- аналіз стартап-проекту

Сильні сторони: економічна (ціна товару).	Слабкі сторони: ступінь задоволення потреб користувача, якість розробки з точки зору оптимальності показників надійності.
Можливості: знижувати витрати на виробництво продукції, покращувати якість та надійність продукту; формування попиту у користувачів за рахунок покращення характеристик товару.	Загрози: потрібно знайти людей з певними навичками і знаннями і запропонувати вигідні умови для співпраці; технічне забезпечення та спеціальні умови для перевірки працездатності продукту.

На основі SWOT-аналізу розробляються альтернативи ринкової поведінки (перелік заходів) для виведення стартап-проекту на ринок та орієнтовний оптимальний час їх ринкової реалізації з огляду на потенційні проекти конкурентів, що можуть бути виведені на ринок (див. табл. 3.9, аналіз потенційних конкурентів). Визначені альтернативи аналізуються з точки зору строків та ймовірності отримання ресурсів (табл. 3.13).

Таблиця 3.13 – Альтернативи ринкового впровадження стартап-проекту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1.	Дослідження поведінки споживачів, пошук наукових ресурсів, розробка обладнання, створення реклами, взаємодія з покупцями для перевірки працездатності обладнання	60%	1 рік
2.	Дослідження поведінки споживачів, пошук інвесторів, пошук наукових ресурсів, створення обладнання, тестування	90%	1 рік

Обрано альтернативу № 2.

3.4. Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії своїм першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів (табл. 3.13). Опис цільових груп надає можливість визначити відносну важливість груп та стратегію маркетингу.

Таблиця 3.14 – Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1.	Збройні сили	Готові	Середній	Середня	Середня
2.	ДСНС	Готові	Середній	Середня	Середня
3.	Цивільні піротехніки	Готові	Середній	Висока	Середня
Які цільові групи обрано цільову групу №1, №2 та №3					

Після проведеного аналізу цільових груп було обрано стратегію масового маркетингу

Для роботи в обраних сегментах ринку необхідно сформулювати базову стратегію розвитку (табл. 3.15).

Таблиця 3.15 – Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
1.	1	За рахунок великих можливостей по об'ємах збуту товарів і продуктивності підприємство може добитися менших витрат	Витрати на виробництво	Стратегія лідерства на витратах
2.	2	Надання товару важливих з точки зору споживача відмінних властивостей, що роблять товар відмінним від товарів конкурентів. Така відмінність може базуватися на об'єктивних або суб'єктивних, відчутних і невідчутних властивостях товару бути реальним або уявним.	Формування попиту у користувачів за рахунок спеціального функціоналу та високої якості товару	Стратегія диференціації
3.	3	Концентрація на потребах одного цільового сегменту, без прагнення охопити увесь ринок. Низька ринкова доля у разі невдалої реалізації стратегії може істотно підірвати конкурентоспроможність компанії.	Задоволення потреб вибраного цільового сегменту краще, ніж конкуренти.	Стратегія спеціалізації

Обрано стратегію диференціації. Наступним кроком є вибір стратегії конкурентної поведінки (табл. 3.16).

Таблиця 3.16 – Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект "першо-прохідцем" на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки*
1.	Ні	Так	Так, основний функціонал	Наслідкування лідера

На основі вимог споживачів з обраних сегментів до постачальника (стартап-компанії) та до продукту (табл. 3.5), а також в залежності від обраної базової стратегії розвитку (табл. 3.15) та стратегії конкурентної поведінки (табл. 3.16) розробляється стратегія позиціонування (табл. 3.17). що полягає у формуванні ринкової позиції (комплексу асоціацій), за яким споживачі мають ідентифікувати торгівельну марку/проект.

Таблиця 3.17 – Визначення стратегії позиціонування

№ п/п	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
1.	Товар має бути надійним та зручним у використанні.	Диференціації	Низька ціна, висока надійність, простий та зрозумілий інтерфейс керування, високий функціонал	Оптимальне співвідношення ціна/якість, наукоємність, надійність

3.5 Розроблення маркетингової програми стартап-проекту

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього у табл. 3.18 наведені результати попереднього аналізу конкурентоспроможності товару.

Таблиця 3.18 – Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
1.	Можливість розширення радіусу дії	Можливість підключення повторювачів	Зручність використання
2.	Надійність	Використання надійних елементів та обладнання	Стабільність роботи

Надалі розробляється трирівнева маркетингова модель товару: уточнюється ідея продукту та/або послуги, його фізичні складові, особливості процесу його надання (табл. 3.19).

Таблиця 3.19 – Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові		
I. Товар за задумом	Засоби розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів		
II. Товар у реальному виконанні	Властивості/характеристики	М/Нм	Вр/Тх /Тл/Е/Ор
	1. Низька ціна 500 грн 2. Сумісність з більшістю електровибухового та піротехнічного обладнання 3. Можливість збільшувати робочу відстань 3. Висока надійність 5. Безпечність користування	М М М М М	
	Якість: висока функціональність та якість		
	Пакування: невелика коробка		

	Марка: "Мій проект"
III. Товар із підкріпленням	До продажу: гарантія
	Після продажу: доставка, обслуговування, налаштування
За рахунок чого потенційний товар буде захищено від копіювання: захист інтелектуальної власності	

Після формування маркетингової моделі товару слід особливо відмітити – чим саме проект буде захищено від копіювання. Захист може бути організовано за рахунок захисту ідеї товару (захист інтелектуальної власності), або ноу-хау, чи комплексне поєднання властивостей і характеристик, закладене на другому та третьому рівнях товару.

Наступним кроком є визначення цінових меж, якими необхідно керуватись при встановленні ціни на потенційний товар (остаточне визначення ціни відбувається під час фінансово-економічного аналізу проекту), яке передбачає аналіз ціни на товари-аналоги або товари субституту, а також аналіз рівня доходів цільової групи споживачів (табл. 3.20). Аналіз проводиться експертним методом.

Таблиця 3.20 – Визначення меж встановлення ціни

№ п/п	Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
1.	—	2000...10000 грн	30000 грн і вище	500 – 700 грн

Наступним кроком є визначення оптимальної системи збуту, в межах якого приймається рішення. Так як товар є специфічним, то збут має проводитись власними силами до тендерних відділів збройних сил та спеціальних служб, а також можливий збут через посередників, а саме через магазини піротехнічного обладнання, при збуті цивільним особам.

Висновки

На сьогодні засоби розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів є актуальними, адже наразі у світі відбувається багато військових конфліктів, після яких треба зробити безпечними великі території, на яких залишилися боєприпаси. Застарілі пристрої для знешкодження вибухонебезпечних предметів є габаритними та не контролюються безпроводно, тому не є доцільними у використанні.

На українському ринку зараз немає значної конкуренції в даному напрямі. Більшість аналогів мають високу вартість та спеціалізовані лише під піротехнічну справу, також не мають можливості значно збільшити робочу відстань.

Для впровадження доцільно обрати альтернативу дослідження поведінки споживачів, пошук інвесторів, пошук наукових ресурсів, створення обладнання, тестування

Подальше виконання проекту безперечно є доцільне.

4. ОБГРУНТУВАННЯ СТРУКТУРИ ТА СХЕМИ ЗАСОБУ РОЗШИРЕНОГО РАДІУСУ ДІЇ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ Wi-Fi ДЛЯ ЗНЕШКОДЖЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

4.1 Обґрунтування структурної схеми системи

Проаналізувавши та детально розглянувши технічне завдання можна перейти до етапу розробки структурної схеми засобів розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів

Виходячи із отриманого завдання, пристрій повинен виконувати наступні функції:

- 1.) забезпечення ефективної роботи на відстані;
- 2.) спрацювання електродетонатору через резервний вивід;
- 3.) обробка отриманої інформації;
- 4.) швидке спрацювання;
- 5.) зручність використання;
- 6.) можливість збільшення робочої відстані.

Центральним органом керування системи є МК. За допомогою нього узгоджуються всі дії та функції. Сформовано структурну схему системи, яка приведена на рисунку 4.1.



Рисунок 4.1 – Структурна схема пристрою ЗВНП з керуванням через канал Wi-Fi

На рисунку 4.1. зображено структурну схему ЗЗВНП, яка складається з таких блоків:

- 1) блок живлення;
- 2) мікроконтролер;
- 3) блок вводу інформації;
- 4) реле;
- 5) безпроводний інтерфейс.

Блоком вводу інформації може слугувати як передаючий пристрій, так і повторювач.



Рисунок 4.2 – Структурна схема повторювача

На рисунку 4.2. зображено структурну схему повторювача, яка складається з таких блоків:

- 1) блок живлення;
- 2) мікроконтролер;
- 3) блок вводу інформації;
- 4) безпроводний інтерфейс.

Вище було зазначено, що мікроконтролер виконує функцію взаємодії між усіма блоками пристрою, які вказані на структурних схемах. Керування забезпечується відповідним програмним забезпеченням для мікроконтролера. Основним інтерфейсом взаємодії з користувачем є блок вводу інформації.

4.2. Обґрунтування та вибір елементної бази

Важливим етапом у процесі конструювання є вибір та обґрунтування елементної бази. На цьому етапі треба обирати оптимальний варіант елементної бази серед всіх розглянутих варіантів за необхідними параметрами.

В розділі 1.7 було наведено 7 різних Wi-Fi модулів, серед них було обрано модуль серії ESP8266, адже він не потребує використання додаткового зовнішнього мікроконтролера та має низьку вартість.

У системі будуть присутні декілька мікросхем. Приклад розрахунку буде проводитись на основі головної мікросхеми – мікроконтролера. При виборі мікроконтролера для пристроїв було сформовано список найбільш застосовуваних, для подібного типу задач. Параметри мікроконтролерів приведені в таблиці 4.1.

Таблиця 4.1. Основні параметри МК

Параметри				
Модель	Порти в/в (шт)	Частота F_{max} (МГц)	Об'єм пам'яті (кБ)	Вартість (грн.)
ESP8266-01	4	80	64	79
ESP8266-07	7	80	80	88
ESP8266-12E	9	80	80	85
ESP32	13-31	240	520	230

З отриманих вище даних висновком може слугувати те, що кращим МК для використання буде ESP8266-01, адже в нього достатньо пам'яті та портів вводу-виводу для розроблюваного пристрою, а також він має найменші розміри. Але він є недостатньо надійним, при увімкненні МК наявні сигнали на всіх його виводах, тому в цілях безпеки обрано ESP8266-12E. Цей МК є найкращим варіантом для вирішення поставлених задач, так як він задовольняє всі вимоги, що поставлені до пристрою, та додати резервні виводи. Таким же чином обрані інші компоненти системи.

На рисунку 4.3 наведено призначення портів ESP 8266-12E, а саме:

RST – призначений для перезавантаження модуля;

ADC – вхід аналого-цифрового перетворювача;

EN – для переведення в енергозберігаючий режим;

GPIO – порти виведення;

VCC – для подачі живлення;

TXD0 – апаратний UART інтерфейс;

RXD0 – апаратний UART інтерфейс;

GND – заземлення;

CS0 – вибір чіпу;

MISO – вхід провідного, вихід веденого;

MOSI – вхід веденого, вихід провідного;

SCLK – послідовний тактовий сигнал.

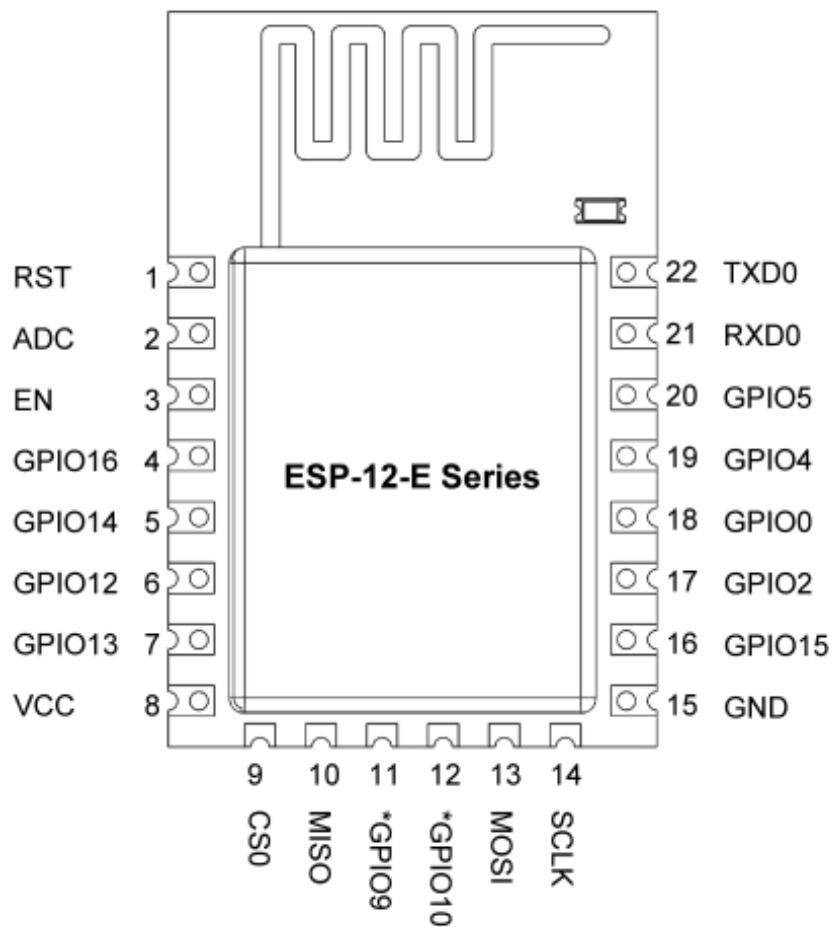


Рисунок 4.3 – Призначення портів ESP 8266-12E

4.3 Особливості схеми електричної принципової

Відповідно до структурної схеми, яка зображена на рисунку 4.3 необхідно розробити схему електричну принципову, яка повинна відповідати функціям наведеним у підрозділі 4.1.

Основою пристрою (рис. 4.4) є мікроконтролер фірми Espressif ESP 8266-12E з модулем Wi-Fi, який має 512 кБайт Flash — пам'яті, 80 кБайт RAM пам'яті, , UART, SDIO та SPI модулі.

Мікроконтролер має живлення 3.3 В (Вивід VCC). При стандартному підключенні виводи GPIO15 та GND підключають між собою. Для підвищення ефективності роботи вивід CH_PD підключають до 3.3V через резистор 10кОм, також виводи RESET, GPIO (0, 2) з'єднують з 3,3V резисторами 10 кОм., До виводів живлення під'єднують електролітичний конденсатор на 100-220 мкФ та керамічний на 0.1 мкФ задля подавлення завад. Короткочасне замикання RST на GND призводить до перезавантаження модуля.

На схемі обрано інший тип підключення: GPIO15 через резистор 10 кОм підключено на землю, виводи RXD та TXD під'єднано до стабілізатора напруги через резистори 100 Ом, REST підведено до землі через ключ.

Блоком управління пристроєм є смартфон.

Пристроєм передбачено підключення до 5 реле.

Додатково до входних контактів реле K1–K5 увімкнено діоди VD1 – VD5 для запобігання протікання зворотнього струму, при відключенні котушки реле.

Основою повторювача (рис. 4.5) також є мікроконтролер фірми Espressif ESP 8266-12E з модулем Wi-Fi. Схема повторювача дублює схему кінцевого пристрою, але не включає в себе каскад реле, натомість може містити додаткову антену.

Перелік елементів кінцевого пристрою наведено в таблиці 4.2. Перелік елементів повторювача наведено в таблиці 4.3.

Таблиця 4.2 – Перелік елементів кінцевого пристрою

Позначення	Найменування	Кількість
C1	Конденсатор ELZET 10 мкФ	1
C2	Конденсатор ELZET 22 мкФ	1
R1, R2	Резистор SMD YAGEO 100 Ом	2
R3	Резистор SMD YAGEO 100 кОм	1
DA1	Стабілізатор AMS1117	1
DA2	Перетворювач USB-UART CP2102	1
DD1	Модуль ESP 8266-12E	1
VD1-VD5	Діод 1N4154	5
K1-K5	Реле Zettler AZ850-3	5

Таблиця 4.3 – Перелік елементів повторювача

Позначення	Найменування	Кількість
C1	Конденсатор ELZET 10 мкФ	1
C2	Конденсатор ELZET 22 мкФ	1
R1, R2	Резистор SMD YAGEO 100 Ом	2
R3	Резистор SMD YAGEO 100 кОм	1
DA1	Стабілізатор AMS1117	1
DA2	Перетворювач USB-UART CP2102	1
DD1	Модуль ESP 8266-12E	1

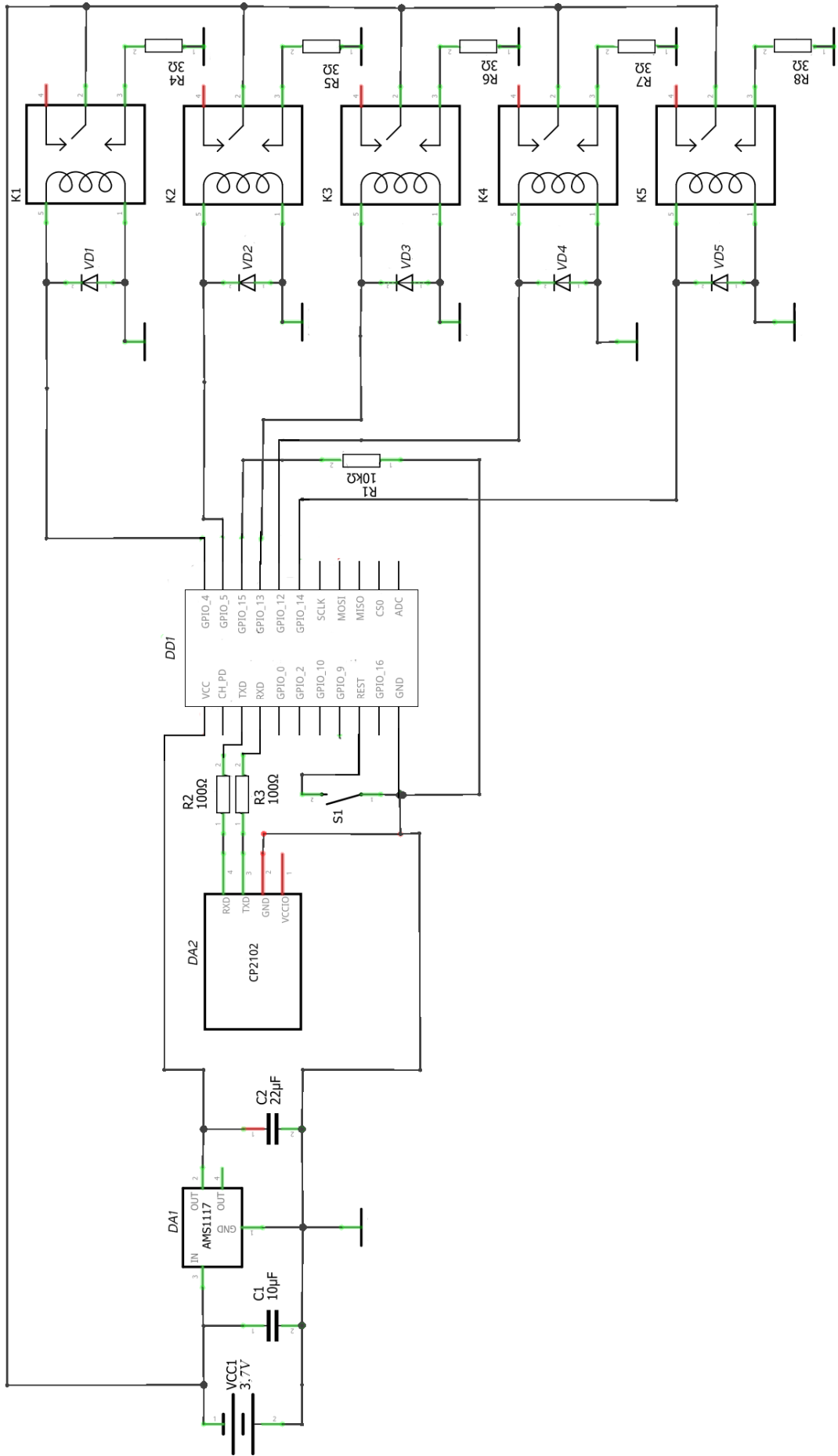


Рисунок 4.4 – Схема електрична принципова кінцевого пристрою

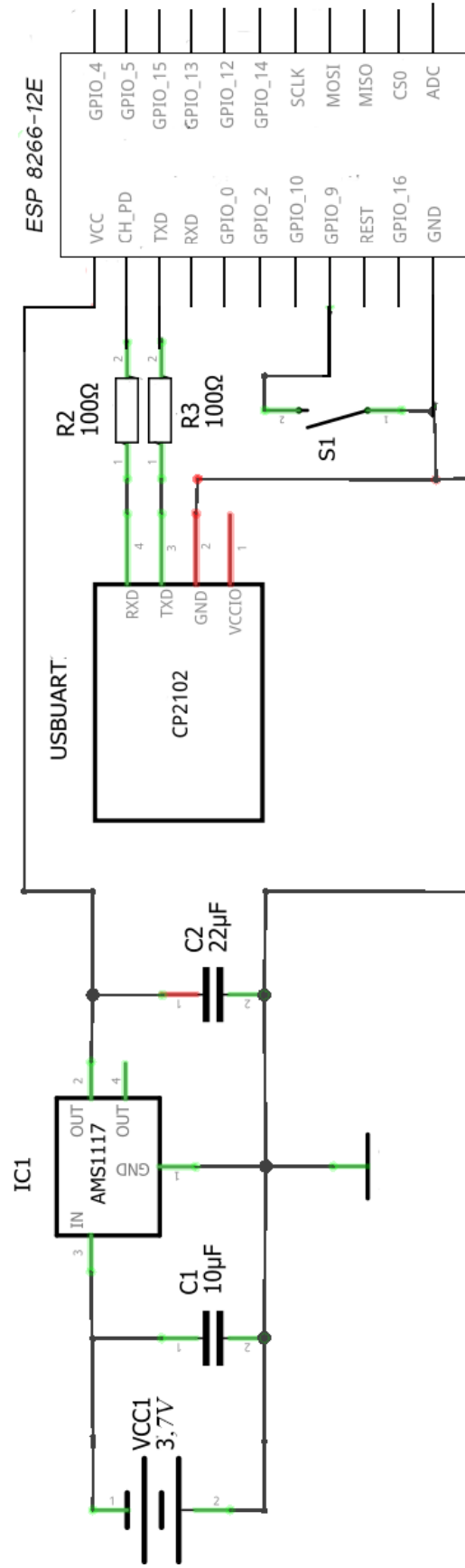


Рисунок 4.5 – Схема електрична принципова повторювача

4.4. Програмна реалізація та моделювання роботи системи

4.4.1. Обґрунтування алгоритму роботи програми

Зазвичай будь – яка система складається з програмного забезпечення. Інтерфейс взаємодії системи з користувачем повинен бути достатньо простим у використанні. На рисунку 4.6 наведено алгоритм роботи програми засобу розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів.

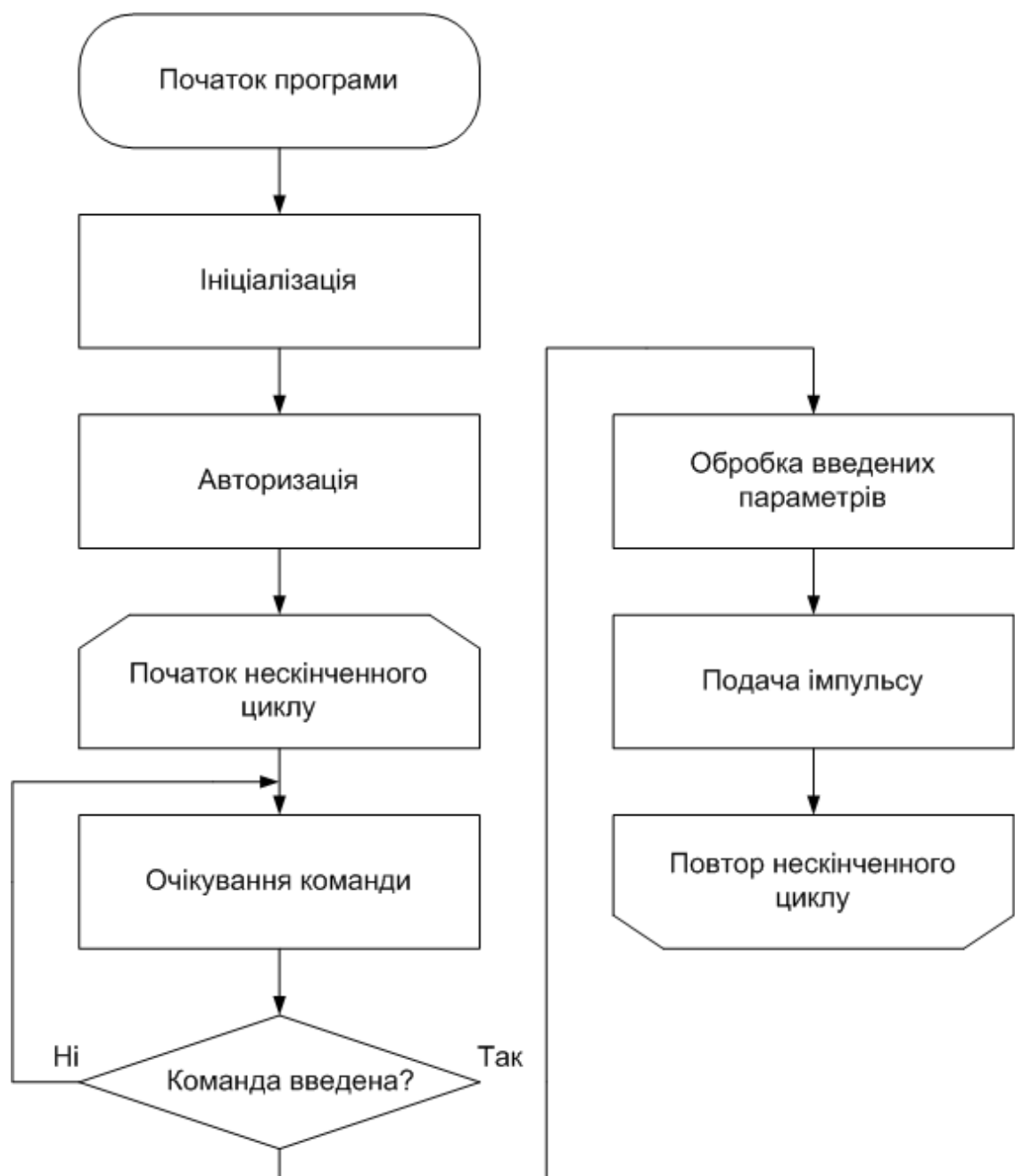


Рисунок 4.6 – Алгоритм програми кінцевого пристрою

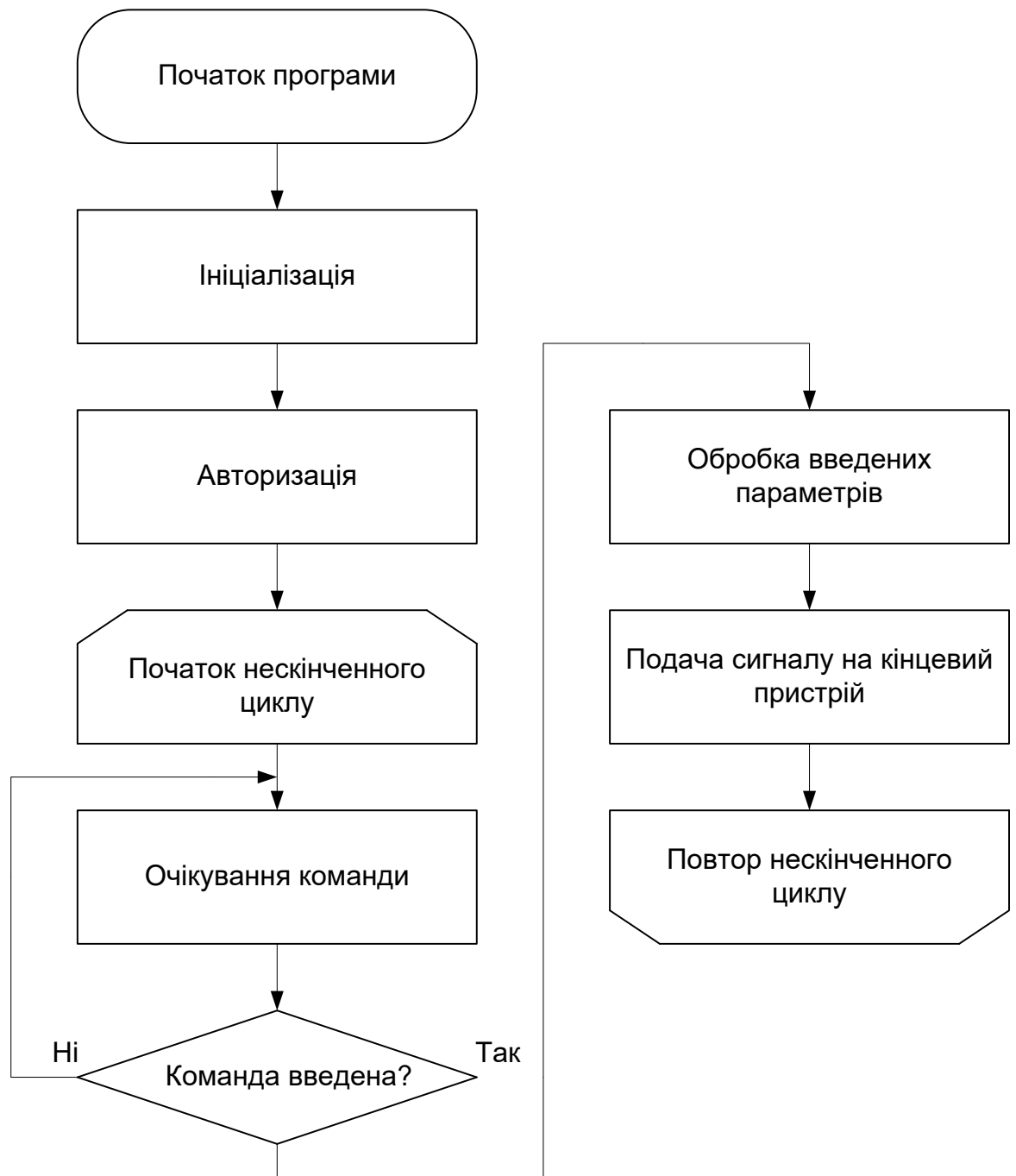


Рисунок 4.7 – Алгоритм програми повторювача

4.4.2. Опис роботи програмного забезпечення засобу для знешкодження вибухонебезпечних предметів

Мікроконтролер ESP8266 програмується на мові C++, LUA або AT-командами. Найбільш зручним є варіант програмування на мові LUA та з

використанням середовища ESPlorer. Тому програмне забезпечення даного пристрою розроблене мовою LUA.

LUA — швидка і компактна скриптова мова програмування. Є вільно-поширюваною з відкритими вихідними кодами на мові C.

За можливостями, ідеологією і реалізацією, мова найближча до JavaScript, проте Lua відрізняється потужнішими і набагато гнучкішими конструкціями, спроектованими з метою «не плодити сутності понад необхідне». Хоча Lua не містить поняття класу і об'єкта в явному вигляді, механізми об'єктно-орієнтованого програмування з підтримкою прототипів (включаючи множинне успадкування) легко реалізуються з використанням метатаблиць, які також дозволяють перевантаження операцій, тощо. Реалізована модель ООП (як і в JavaScript) — прототипна.

Lua комбінує простий процедурний синтаксис з потужними можливостями опису даних через використання асоціативних масивів і розширюваної семантики мови. У Lua використовується динамічна типізація, мовні конструкції перетворюються в байт-код, який виконується поверх регістрової віртуальної машини з автоматичним збирачем сміття. Сам інтерпретатор оформлений у вигляді бібліотеки, легко інтегрованої в проекти на мовах C та C++. Код інтерпретатора Lua написаний на мові C і розповсюджується під ліцензією MIT.

Робота програми повторювача розпочинається з підключення до серверу, що знаходиться у пам'яті мікроконтролера, ініціалізації та авторизації оператора. Повторювач працює в режимі сервер-точка доступу.

Після авторизації користувача, можна приступати к використанню пристрою. Сервер очікує команду, а після її отримання передає сигнал на кінцевий пристрій.

Робота програми кінцевого пристрою заключається в тому, що він підтримує зв'язок з повторювачем, після отримання команди з нього, кінцевий пристрій подає імпульс на відповідне реле.

4.5. Особливості друкованої плати для засобу знешкодження вибухонебезпечних предметів

4.5.1. Вибір типу друкованої плати

Типи друкованих плат:

- односторонні ДП (ОДП);
- двосторонні ДП (ДДП);
- багатошарові ДП (БДП);
- гнучкі ДП (ГДП);
- гібридні ДП (ГДП).

ОДП є простими й економічними у виготовленні. Вони забезпечують можливість виконання провідників з підвищеною точністю. Дозволяють здійснювати встановлення навісних елементів на поверхню плати зі сторони, протилежній пайці, без додаткової ізоляції.

ДДП поділяють на 2 групи: плати з металізацією і без металізації наскрізних отворів. Плати без металізації через наявність ще одного шару (в даному випадку - першого) підвищується трасувальна здатність ДП і певною мірою щільність монтажу елементів. Проблема таких плат це — забезпечення електричних переходів між шарами, для чого застосовуються заклепки, проводові перемички і т. д. Це істотно підвищує складність монтажу і вартість пристрою. Плати з металізацією - перехідних отворів також мають високу трасувальну здатність, забезпечують високу щільність монтажу елементів і хорошу механічну міцність їх закріплення. Ці ДП допускають монтаж елементів на поверхню і є найбільш поширеними у виробництві радіоелектронних пристроїв.

БДП складаються з шарів які чергуються з ізоляційних матеріалів і провідників, з'єднаних прокладками в багатошарову структуру шляхом пресування.

БДП характеризують підвищеною щільністю монтажу, стійкістю до механічних і кліматичних впливів, складністю технології виготовлення і конструювання, високою вартістю

ГДП (гнучкі та гібридні) - згорнуті в рулон плати. ГДП: компактні, надійні, ударостійкі. Головний недолік ГДП — висока вартість матеріалів для їх виготовлення.

Для розроблюваного пристрою обрано двосторонню ДП. Застосування ДДП достатньо для реалізації усіх необхідних функцій пристрою, також через низьку вартість плат такого типу вона підходить найбільше.

4.5.2. Вибір матеріалу друкованої плати

Матеріалами для виготовлення ДП є діелектрики, найчастіше гетинакс і склотекстоліт. Гетинакс — складається з пресованих шарів електроізоляційного паперу, які просочені фенольною смолою. Склотекстоліт — складається з пресованих шарів склотканини, які просочені епоксидною смолою. Склотекстоліт краще гетинаксу за всіма електромеханічним параметрам, але його вартість вища .

Для розроблюваного пристрою було прийнято рішення вибрати фольгований склотекстоліт, адже висока вірогідність того, що пристрій буде використовуватись в екстремальних умовах.

4.5.3. Виготовлення друкованих плат

Відома велика кількість технологічних варіантів виготовлення друкованих плат. Найбільш широкого поширення набули наступні методи:

- хімічний метод. Полягає в тому, що на мідну фольгу, приклеєну до діелектрика, наносять кислотостійкою фарбою малюнок

розташування друкованих провідників. Травління видаляється мідь з незахищених ділянок і на діелектриці залишається схема провідників. Найбільш поширеними варіантами цього способу є фотохімічний, сітчасто-хімічний, офсетно-хімічний, які розрізняються способом нанесення захисного шару;

- електрохімічний метод. Полягає в нанесенні на плату кислотостійкою фарбою негативного малюнка провідників. Нанесення малюнка відбувається з наступним нарощуванням шару міді;
- комбінований метод. Полягає в отриманні провідників шляхом травління фольгованого діелектрика і металізацією отворів електрохімічним способом.

Після механічної обробки плата перевіряється на наявність тріщин на краях плати і в отворах, відшаровування друкованих провідників в зоні отворів. Друковані провідники мають бути чіткими. Цілісність електричних кіл встановлюється методом прозвонки.

Деталі на плату встановлюють вручну, пайку монтажних з'єднань виконують паяльником потужністю 35 Вт та припоєм ПОС-60. Застосовують тільки безкислотні флюси. Якість пайки перевіряють зовнішнім оглядом. Для захисту провідників і поверхні основи плати від дії припою використовують резистивні маски на основі епоксидної смоли, сухого плівкового резисту. Для виготовлення плати обрано комбінований метод.

Ширина плати кінцевого пристрою — 72 мм;

Довжина плати кінцевого пристрою — 105 мм;

Ширина плати повторювача — 72 мм;

Довжина плати повторювача — 83 мм.

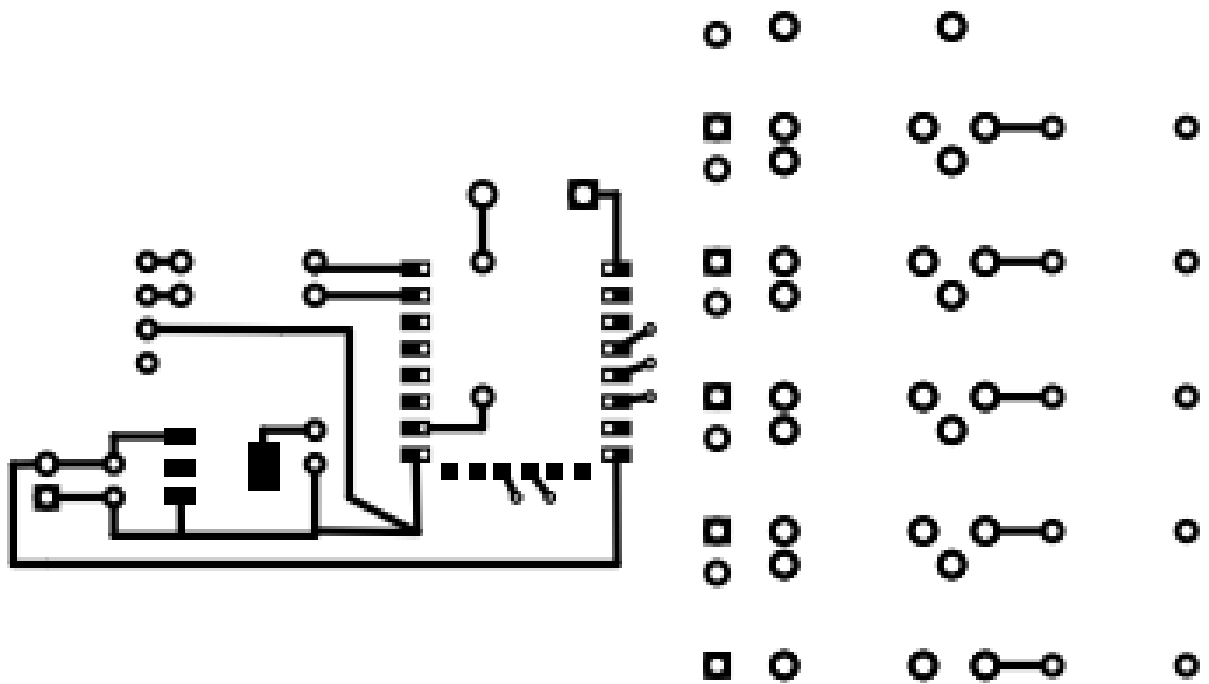


Рисунок 4.8 – Друкована плата кінцевого пристрою верхній шар

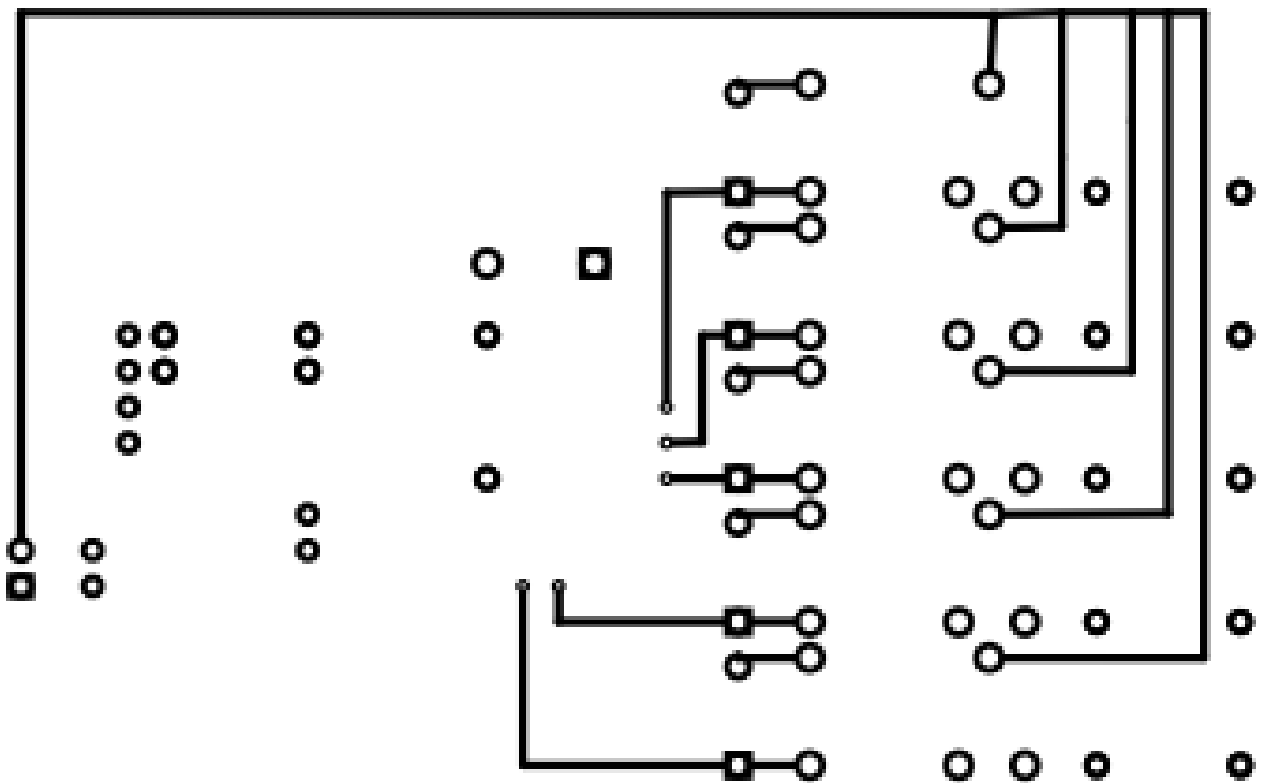


Рисунок 4.9 – Друкована плата кінцевого пристрою нижній шар

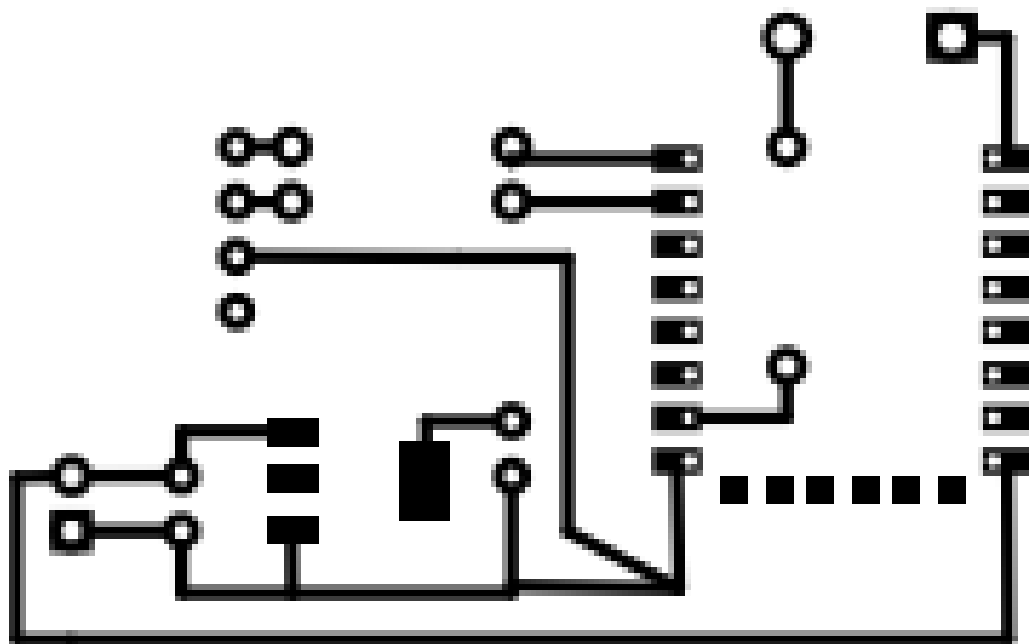


Рисунок 4.10 – Друкована плата повторювача

Висновки:

В розділі було описано структурну схему, обрано та описано елементну базу пристрою для знешкодження вибухонебезпечних предметів, були наведені особливості електричної принципової схеми, обґрунтовано вибір друкованої плати та наведено алгоритм роботи програми пристрою.

Система складається з кінцевого пристрою та півторювача. В кінцевий пристрій входить мікроконтролер, блок введення інформації, блок живлення та каскад реле. В повторювач входить мікроконтролер, блок введення інформації та блок живлення.

Програмне забезпечення пристрою створене за допомогою мови LUA. Друкована плата була обрана двостороння з фольгованого текстоліту.

ВИСНОВКИ

Метою даної магістерської дисертації є вдосконалення засобів розширеного радіусу дії із застосуванням технології Wi-Fi для знешкодження вибухонебезпечних предметів. В результаті вирішення поставлених задач, було досягнуто таких результатів:

1. Проведено аналіз існуючих пристроїв, який показав, що дана тема є актуальною на сьогоднішній день. Актуальність полягає у створенні нових та модернізації старих пристроїв з метою зменшення їх собівартості, габаритів та підвищення зручності керування, а також рівня безпеки.

2. Проаналізувавши характеристики пристрою, було визначено основні параметри, що можливо покращити, обрано діапазон покращень та шляхи. Основними параметрами є радіус дії та надійність. Задля покращення радіусу дії було обрано шлях встановлення зовнішньої антени та використання повторювачів в лінії зв'язку. Для покращення надійності потрібно використовувати якісні технічні засоби та матеріали.

3. Обґрунтовано вибір елементної бази та структурну схему пристрою.

На основі обраної елементної бази для засобу знешкодження вибухонебезпечних предметів було розроблено схему електричну принципову, з урахуванням рекомендацій вказаних в технічній документації елементів.

4. Проведено аналіз типів і матеріалів, які використовуються при виготовленні друкованих плат. Обрано двосторонню друковану плату з склотекстоліту марки СФ – 2 – 35 – 1.5 ГОСТ 10316 – 78, так як вона має високі показники надійності. Обрано четвертий клас точності, за допомогою якого досить компактно розміщено елементи. Обраній елементній базі співставлено корпуси виконання. Виявлено, що для виготовлення друкованої плати більш доцільним буде використання комбінованого позитивного методу. Плата відповідає технічним вимогам четвертого класу точності.

Виконано електричний розрахунок друкованої плати, який показав наступні результати:

- спад напруги на найдовшому провіднику: 0.24 В;
- потужність втрат друкованої плати: 2.1 мкВт.

Для мікроконтролера ESP 8266-12E не потрібно встановлювати додаткові засоби охолодження.

5. Наведено алгоритм програмного забезпечення для системи, описано принцип роботи програми, що використовується у кінцевому пристрої та програми, що повторювача.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Эпов Б.А. Основы взрывного дела. Пособие / Эпов Б. А. – М.: Военное издательство министерства обороны, 1974 . – 227 с.
2. Производство взрывных работ при проведении аварийно-спасательных и других неотложных работ в различных чрезвычайных ситуациях. / [Гребенюк А. М., Одинцов Л. Г., Васильев В. А., Шеломенцев С. В.]. – М.: Научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций, 2006. – 203 с.
3. Основи інформаційних систем: Навчальний посібник. / [В. Ф. Ситник, Т. А. Писаревська, Н. В. Єрємін, О. С. Краєва;]. – К.: КНЕУ, 2001. – 420 с.
4. Надійність електронних систем. / [Пацюра І.В., Корнейчук В.І., Довбиш Л.В.] – К.: Світ, 1997. – 128 с.
5. Ильин В.А. Технология изготовления печатных плат/ Ильин В.А. – Л.: Машиностроение, Ленингр. отд-е, 1984. – 77 с.
6. Микропроцессоры / Самофалов К.Г., Викторов О.В. – К.: Техника, 1989. – 312 с.
7. Белов А.В. Конструирование устройств на микроконтроллерах / Белов А.В. – СПб.: Наука и техника, 2005. – 256 с.
8. Технология деталей радиоэлектронной аппаратуры. Учебное пособие для вузов. / Ушакова С. Е., Сергеев В. С. - М.: Радио и связь, 2002. – 256 с.
9. Espressif [URL] – <https://www.espressif.com>
10. Сообщество ESP 8266 [URL] – <https://esp8266.ru/forum/>
11. Технологии беспроводной передачи данных [URL] – http://wireless-e.ru/articles/bluetooth/2006_1_10.php
12. Подрывная машинка [URL] – <http://enciklopediya-tehniki.ru/promyshlennost-na-p/podryvnaya-mashinka.html>
13. Жуков Н. Средства поиска и обезвреживания взрывоопасных предметов// Зарубежное военное обозрение, 1993, 9. - С.23.

14. Пролетарский А. В., Баскаков И. В., Чирков Д. Н. Беспроводные сети./ Пролетарский А. В. – М: издательство Бином, 2007. – 1
15. Калачев А. Беспроводные приложения: план действий, компоненты Texas Instruments – и вперед! / А. Калачев. – М. : Новости электроники, 2011. – №4. – с. 12-19.
15. Б. С. Гершунский. Справочник по расчету электронных схем / Б. С. Гершунский. – К. : Вища школа, 1983. – 240 с.
16. Семенов Б. Ю. Силовая электроника для любителей и профессионалов / Б. Ю. Семенов. – М. : СОЛОН-Р, 2001. – 334 с.
17. Розроблення стартап-проекту [URL] : Методичні рекомендації до виконання розділу магістерських дисертацій для студентів інженерних спеціальностей / За заг. ред. О.А. Гавриша. – Київ : НТУУ «КПІ», 2016. – 28 с.
18. ДСТУ 3008:2015. Національний стандарт України: Інформація та документація. Звіти у сфері науки і техніки, структура і правила оформлювання, Київ – 2016.

ДОДАТОК А
ABSTRACT

During widespread military conflicts, the topic of the development of technical measures aimed at overcoming the consequences of hostilities, namely the destruction of non-functioning ammunition in areas with civilian population, is an urgent issue. With the development of modern technology, it is not rational to use outdated blasting machines, which is very large, but the best option is to use small-sized microcontroller assemblies and wireless technologies such as Wi-Fi.

The use of Wi-Fi technology is advisable because it is possible to control the device from any device with a Wi-Fi module, such as smartphones, laptops, tablets, and the like. Also, such devices do not require large antennas due to short wavelengths.

The operation of the remote disposing of explosive objects is based on the principle of transmitting a signal from the command-transmitter to the receiver-actuator, which initiates the current pulse on the electrodetonator.

The most important device criteria is the range and size. In this case, it is advisable to use powerful transmitter devices and try to reduce the size of the device.

One of the main characteristics of a device for the clearance of explosive items is reliability. Therefore, a microcontroller, which has a copy of the main parameters of the system in the independent memory, a large number of outputs, etc. is selected. In addition to the controller, the device for the clearance of explosive items includes a Wi-Fi module, antenna and relay kit.

The distance of the normal operation of the devices depends on the transmitter power, the presence of antennas, amplifiers, relief and geomagnetic conditions. The downside of Wi-Fi technology is a small amount of action that can be corrected, added to the line of amplifiers and a more powerful antenna.

In microcontrollers with a Wi-Fi module, such as Espressif ESP's lineup, printed antennas operate at distances of up to 350 meters, but for expanding the range, it is possible to install an external additional antenna, which increases the working distance to 480 meters. It is also possible to use the line the transmission of additional devices that will receive the control signal and transmit it to the terminal device.

One more factor of relevance and expediency of using devices with microcontrollers and wireless technologies is the possibility of joining them into one network, which enables them to be activated in any order and at any time. Also, one end device may have the number of outputs required by the task.

The prevalence of microcontrollers in the market provides a wide choice, low cost and sufficient reliability. The cost of this type of equipment will not be much higher than the cost of outdated blasting machines.

The principle of the job is that the device acts as a server and contains in its memory an executable program, the control takes place remotely from a smartphone, laptop or tablet, the method of connecting to the server, and the launch of the program, after which the device gives a pulse of current to the selected output and initiates an electrodone detector.

The analysis of the market showed that it presents a narrow range of devices for the elimination of explosive objects, most of which have infiltrated, as well as no solutions with wireless control.

Extensive measures with the use of Wi-Fi technology for the clearance of explosive items can be used to test new electrical equipment (electric detonators), not only in military affairs, but also in civilian pyrotechnic events, launch of fireworks, fire control equipment testing, etc.

The purpose of this master's thesis is to develop expanded range of devices using Wi-Fi technology for the elimination of explosive items, in which the issue of creating a new type of device, by combining explosive devices and remote control devices, and also increasing the radius of such devices, was addressed first of all. .

The task is to investigate the feasibility and implementation of the wireless remote control interface of the device for the clearance of explosive objects at a safe distance. The purpose of this master's thesis is to improve the means of expanded range using Wi-Fi technology to eliminate explosive objects. As a result of solving the tasks, the following results were achieved:

1. An analysis of existing devices was carried out, which showed that this topic is relevant to the present day. Relevance is the creation of new and upgrading old devices to reduce their cost, size and ease of management, as well as security.

2. After analyzing the characteristics of the device, the main parameters that could be improved were identified, a range of improvements and paths were chosen. The main parameters are the range and reliability. In order to improve the range, the path for installing an external antenna and the use of amplifiers in the communication line were chosen. To improve reliability, you need to use high-quality hardware and materials.

3. The choice of the element base and the structural scheme of the device is substantiated.

On the basis of the selected elemental base for the device for the elimination of explosive objects, a scheme of electric principles was developed, taking into account the recommendations of the elements specified in the technical documentation.

4. The analysis of types and materials used in the manufacture of printed circuit boards is carried out. Two-sided printed circuit board made of fiberglass made of SF-2 - 35-1.5 GOST 10316-78 is selected, as it has high reliability. The fourth class of accuracy was chosen, with the help of which elements are relatively compact. The selected element base is matched to the shells of execution. It has been found out that the use of the combined positive method would be more expedient to make a printed circuit board. The board meets the technical requirements of the fourth grade of accuracy.

An electrical calculation of the printed circuit board was performed, which showed the following results:

- voltage drop on the longest conductor: 0.24 V;
- The power loss of the PCB: 2.1 μ W.

For an ESP 8266-12E microcontroller, no additional cooling devices are required.

5. The algorithm of the software for the system is given, the principle of the program used in the terminal device and the program of the amplifier is described.

ДОДАТОК Б
ЛІСТИНГ

Лістинг програми кінцевого пристроя:

```
wifi.setmode(wifi.SOFTAP)
wifi.ap.config({ssid="KP",pwd="Korotkov"})
gpio.mode(1, gpio.OUTPUT)
gpio.mode(2, gpio.OUTPUT)
69
gpio.mode(3, gpio.OUTPUT)
gpio.mode(4, gpio.OUTPUT)
gpio.mode(5, gpio.OUTPUT)
srv=net.createServer(net.TCP)
srv:listen(80,function(conn)
conn:on("receive", function(client,request)
local buf = ""
local _, _, method, path, vars = string.find(request, "([A-Z]+) (.+)?(.+) HTTP")
if(method == nil)then _, _, method, path = string.find(request, "([A-Z]+) (.+)
HTTP")
end
local _GET = { } if (vars ~= nil)then for k, v in
string.gmatch(vars,"(%w+)=(%w+)&*" ) do _GET[k] = v
end
end
buf = buf.."<h1> Обрати пеле <h1>
<form src=\"/\">1 <select name=\"pin\" onchange=\"form.submit()\">
local _on,_off = "","" if(_GET.pin == "ON")then
_on = " selected=true"
gpio.write(1, gpio.HIGH)
elseif(_GET.pin == "OFF")then
_off = " selected=\"true\"
gpio.write(1, gpio.LOW)
<form src=\"/\">2 <select name=\"pin\" onchange=\"form.submit()\">
```

```

local _on,_off = "", ""
if(_GET.pin == "ON")then
  _on = " selected=true"
  gpio.write(2, gpio.HIGH)
elseif(_GET.pin == "OFF")then
  _off = " selected=\\"true\\"
  gpio.write(2, gpio.LOW)
70
end)

<form src=\\\"/\\\">3<select name=\\\"pin\\\" onchange=\\\"form.submit()\\\">
local _on,_off = "", ""
if(_GET.pin == "ON")then _on = " selected=true"
gpio.write(3, gpio.HIGH)
elseif(_GET.pin == "OFF")then _off = " selected=\\"true\\"
gpio.write(3, gpio.LOW)
end)

<form src=\\\"/\\\">4 <select name=\\\"pin\\\" onchange=\\\"form.submit()\\\">
local _on,_off = "", ""
if(_GET.pin == "ON")then
  _on = " selected=true"
  gpio.write(4, gpio.HIGH)
elseif(_GET.pin == "OFF")then
  _off = " selected=\\"true\\"
  gpio.write(4, gpio.LOW)
end)

<form src=\\\"/\\\">5 <select name=\\\"pin\\\" onchange=\\\"form.submit()\\\">
local _on,_off = "", ""
if(_GET.pin == "ON")then _on = " selected=true"
gpio.write(5, gpio.HIGH) elseif(_GET.pin == "OFF")then
  _off = " selected=\\"true\\"

```

```

    gpio.write(5, gpio.LOW)
  end)
end
buf =
buf.."<option".._on..">ON</option><option".._off..">OFF</option></select></f
orm>"
client:send(buf) 71
end)
conn:on("sent", function (c) c:close() end)
end)

```

Лістинг програми повторювача:

```

wifi.setmode(wifi.SOFTAP)
wifi.ap.config({ ssid="KP",pwd="Korotkov" })
wifi.setmode(wifi.STATION)
wifi.sta.config("KP1","Korotkov")
wifi.sta.connect()
print("Looking for a connection")
tmr.alarm(1, 2000, 1, function()
if(wifi.sta.getip()~=nil) then
tmr.stop(1)
print("Connected!")
print("Client IP Address:",wifi.sta.getip())
cl=net.createConnection(net.TCP, 0)
cl:connect(80,"192.168.4.1")
tmr.alarm(2, 5000, 1, function()
end)
else
print("Connecting...")
gpio.mode(1, gpio.OUTPUT)
gpio.mode(2, gpio.OUTPUT)

```



```

gpio.mode(3, gpio.OUTPUT)
gpio.mode(4, gpio.OUTPUT)
gpio.mode(5, gpio.OUTPUT)
srv=net.createServer(net.TCP)
srv:listen(80,function(conn)
conn:on("receive", function(client,request)
72
local buf = ""
local _, _, method, path, vars = string.find(request, "([A-Z]+) (.+)?(.+) HTTP")
if(method == nil)then _, _, method, path = string.find(request, "([A-Z]+) (.+)
HTTP")
end
local _GET = { } if (vars ~= nil)then for k, v in
string.gmatch(vars,"(%w+)=(%w+)&*" ) do _GET[k] = v
end
end
buf = buf.."<h1> Обрати пеле <h1>
<form src=\"/\">1 <select name=\"pin\" onchange=\"form.submit()\">
local _on,_off = "","" if(_GET.pin == "ON")then
_on = " selected=true"
gpio.write(1, gpio.HIGH)
elseif(_GET.pin == "OFF")then
_off = " selected=\"true\""
gpio.write(1, gpio.LOW)
<form src=\"/\">2 <select name=\"pin\" onchange=\"form.submit()\">
local _on,_off = "",""
if(_GET.pin == "ON")then
_on = " selected=true"
gpio.write(2, gpio.HIGH)
elseif(_GET.pin == "OFF")then

```

```

_off = " selected=\true\"
gpio.write(2, gpio.LOW)
end)

<form src=\"/\">3<select name=\"pin\" onchange=\"form.submit()\">
local _on,_off = "", ""
if(_GET.pin == "ON")then_on = " selected=true"
gpio.write(3, gpio.HIGH)
elseif(_GET.pin == "OFF")then_off = " selected=\true\"
73
gpio.write(3, gpio.LOW)
end)

<form src=\"/\">4 <select name=\"pin\" onchange=\"form.submit()\">
local _on,_off = "", ""
if(_GET.pin == "ON")then
_on = " selected=true"
gpio.write(4, gpio.HIGH)
elseif(_GET.pin == "OFF")then
_off = " selected=\true\"
gpio.write(4, gpio.LOW)
end)

<form src=\"/\">5 <select name=\"pin\" onchange=\"form.submit()\">
local _on,_off = "", ""
if(_GET.pin == "ON")then_on = " selected=true"
gpio.write(5, gpio.HIGH) elseif(_GET.pin == "OFF")then
_off = " selected=\true\"
gpio.write(5, gpio.LOW)
end)
end
buf =

```

```
    buf.."<option".."_on..">ON</opton><option".."_off..">OFF</option></select></f
orm>
    "
    client:send(buf)
  end)
  conn:on("sent", function (c) c:close() end)
end)
```